THE RETENTION AND PROCESSING OF COMMUNICATIONS DATA FOR LAW ENFORCEMENT: A CHALLENGE FOR PRIVACY

By Allison M Holmes

DISSERTATION SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS OF THE UNIVERSITY OF KENT FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

Supervised by Professor Dermot Walsh MRIA

With Dr. Sinéad Ring

Kent Law School – University of Kent

Word Count: 97,375

September 2018

ABSTRACT

Law enforcement agencies are dominant end users of information communication technologies. These technologies are not necessarily created for pursuing criminal justice objectives. They are mechanisms that are built, administered, and maintained by private actors for their own purposes and later incorporated into law enforcement processes. They serve an effective role in the investigation, detection, and prosecution of crime, particularly through their collection and processing of relevant data. For the purposes of this thesis, the data at issue concerns the who, where, when, and how of a communication. Broadly classed as 'communications data' this information is readily and consistently available due to technological developments which result in blanket collection and retention, enable easier access, and create opportunities to derive greater meaning from the information through data analysis. The thesis examines the challenges of reconciling privacy with the use of this data in policing by conducting a critical analysis of 'how, and to what extent, do the current legal and policy frameworks governing the retention of, access to, and analysis of communications data by law enforcement, constitute a violation of privacy which requires substantive changes to the legal regime?'.

Employing the approach of Thomas P. Hughes for examining socio-technical systems, the thesis argues that technology and privacy are co-constructed. This is evidenced though the evolution of the technology and the relevant legal and policy factors which contributed to the information communication system's development and acceptance as a policing tool. Three key areas, namely data retention, access to data, and data analysis are used to explore how communications data intersects with law enforcement objectives. Each element of the system is critiqued to assess significant changes in actors and roles, information types, and transmission principles. Utilising Helen Nissenbaum's theory of contextual integrity, it is argued that changes in each of the three key areas represent a *prima facie* violation of informational norms. Where a violation of these norms is identified, it is then evaluated against the perceived benefits of the technology to determine the impact on privacy. The impact on privacy is weighed against the existing legal safeguards in the investigatory powers mechanisms. Examining the privacy interest in a contextual manner allows for the specifics of the technology system to be incorporated into the assessment of the privacy violations.

The thesis concludes that it is insufficient to apply traditional interpretations of privacy to technologies which have fundamentally altered social expectations through the scale/scope of data, the deconstruction of traditional boundaries, the limitation of ephemerality, and changes in technologically mediated presence. Applying a legal framework which does not acknowledge this impact fails to guarantee fundamental privacy rights. A number of recommendations are advanced for reform of the investigatory powers mechanisms to ensure privacy is protected when communications data is utilised by law enforcement.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I have been truly lucky to work with a wonderful supervisory team, without which this thesis would not have been possible. I would like to offer my sincerest thanks to Professor Dermot Walsh to whom I will forever feel indebted. Your advice and assistance throughout the years was invaluable. Thank you for guiding me throughout the PhD process, offering me space to explore on my own, but always making sure that I managed to connect it back to my research. The comments and advice you offered made me a better researcher and a better scholar. I also wish to thank Dr. Sinéad Ring for her encouragement and guidance. The observations and suggestions you offered let me rethink through my ideas and truly polish my work.

I would like to thank the Postgraduate Research Team at Kent, especially Professor Donatella Alessandrini who was there to listen and offer support. I also wish to thank the wonderful PGR administrative staff, particularly Lynn and Karen. I am very appreciative of all the help and assistance you offered throughout the PGR journey.

I will be forever grateful for the support and encouragement of my family and friends throughout this process. To Michele Hartley you are an inspiration. Thank you for enduring my many requests for help and offering your wisdom and assistance in every way possible. Greg Holmes, you truly piqued my interest in this topic from the start. Our many conversations about the area and the concerns it raised made me consider different aspects for my research and I am sure we will continue to debate them for many years to come. I would especially like to thank Adam O'Sullivan who has been there for me and always knows how to make me smile. And to Madeleine Hartley for her unerring support.

To my dear friend Anthony Furlong, thanks for being there for me from the start. I would also like to thank the soon to be Dr. Morris. I owe you my thanks for many reasons, not the least for tolerating our many late night conversations about technology. Your ability to keep me in good spirits (both figuratively and literally) was invaluable.

Thank you to my KLS colleagues, and especially Jess and Tracey, for allowing me to bend their ears and often act as an unhelpful distraction to their own PhD progress. And to my other colleagues at Kent, Eske, Nele, and Daniel, for the many coffees and discussions about PhD life.

TABLE OF CASES

United Kingdom

A v Director of Establishments of the Security Service [2009] EWHC Civ 24.

A v Director of the Security Service [2010] 2 AC 1.

Anisminic v Foreign Compensation Commission [1969] 1 All ER 208.

Barr & Ors v Biffa Waste Services Ltd (No 3) [2011] EWHC 1003.

Belhadj & Ors v Security Service & Ors [2015] UKIPTrib 13_132-H.

British-Irish Rights Watch & Ors (2003) UKIPTrib/01/77.

Chatwani & Ors v NCA [2015] UKIPTrib 15_84_88-CH.

Home Office v Tariq [2011] UKSC 35.

Kennedy v Security Services, GCHQ and the Metropolitan Police Service (2003) UKIPTrib/01/62.

Liberty & Ors v GCHQ & Ors (2014) UKIPTrib 13_77-H 5 Dec 2014.

Liberty v SSHD [2018] EWHC 976.

Parochial Church Council of the Parish of Aston Cantlow, etc. v Wallbank [2004] UKHL 37.

Poplar Housing Association Ltd v Donoghue (2001) 4 All ER 604.

Privacy International v Investigatory Powers Tribunal [2017] EWHC 114.

Privacy International v Investigatory Powers Tribunal [2017] EWCA Civ 1868.

Privacy International v Secretary of State for Foreign and Commonwealth Affairs & Ors [2016] UKIPTrib 15_110CH

Secretary of State for the Home Department v Rehman [2003] 1 AC 153.

Watson v SSHD [2018] EWCA Civ 70.

R (Weaver) v London and Quadrant Housing Trust [2009] EWCA Civ 587.

YL v Birmingham City Council [2007] UKHL 27.

Court of Justice of the European Union

College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer (C-553/07) [2009] ECLI 293.

Digital Rights Ireland v Minister for Communications & Ors and Michael Seitlinger & Ors (Joined Cases C-293/12 and C-549/12) [2014] 2 All ER.

European Court of Human Rights

Leander v Sweden App no 9248/81 (ECtHR, 26 Mar 1987).

Liberty and Others v. the United Kingdom App no 58234/00 (ECtHR, 1 July 2008).

Malone v United Kingdom App No 8691/79 (ECtHR, 2 Aug 1984).

Peck v United Kingdom App no 44647/98 (ECtHR, 28 Jan 2003).

Perry v United Kingdom App no 63737/00 (ECtHR, 17 June 2003).

Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 Dec 2015).

Rotaru v Romania App no 28341/95 (ECtHR, 4 May 2000).

S and Marper v United Kingdom App No 30562/04 and 30566/04 (ECtHR, 4 Dec 2008).

Szabo & Vissy v Hungary App no 37138/14 (ECtHR, 12 Jan 2016).

Weber & Saravia v Germany App no 54394/00 (ECtHR, 29 June 2006).

Foreign Jurisdictions

Court of Cassation (Cour de Cassation), Arrêt No. 1184 du 3 novembre 2016, 15-22.595 [France].

Criminal Chamber of the Supreme Court, no3-1-1-51-14 (23 Feb 2015) [Estonia].

Digital Rights Ireland Ltd v Minister for Communication & Ors [2010] IEHC 221 [Ireland].

Director of Public Prosecutions v Graham Dwyer (2014) CCCD [Ireland].

Kane v Governor of Mountjoy Prison [1988] 1 IR 757 [Ireland].

Riley v California 134 S Ct 2473 (2014) [United States].

TABLE OF LEGISLATION

United Kingdom

Anti-Terrorism Crime and Security Act 2001

British Telecommunications Act 1981

Counter-Terrorism and Security Act 2015.

Court of Session Act 1988

Criminal Procedure and Investigations Act 1996

Data Protection Act 1998

Data Protection Act 2018

Data Retention and Investigatory Powers Act 2014

Digital Economy Act 2017

Human Rights Act 1998

Interception of Communications Act 1985

Investigatory Powers Act 2016

Police Act 1997

Post Office Act 1969

Protection of Freedoms Act 2012

Regulation of Investigatory Powers Act 2000

Tribunals Courts and Enforcement Act 2007

Statutory Instruments

Data Retention and Acquisition Regulations 2018 DRAFT SI 2018.

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

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

Data Retention Regulations 2014, SI 2014/2042.

Investigatory Powers (Review of Notices and Technical Advisory Board) Regulations 2018, SI 2018/354.

Investigatory Powers (Technical Capability) Regulations 2018, SI 2018/353.

Investigatory Powers Tribunal Rules 2000, SI 2000/2665.

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

Regulation of Investigatory Powers (Communications Data) Amendment Order 2015, SI 2015/228.

European Union

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 (1998) OJ L 24.

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

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data in the electronic communications sector (2002) OJ L201

Directive 2006/24/EC 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 2005 (2006) OJ L105.

Directive 2016/680/EC 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016) OJ L119.

Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice (2016) OJ C 202.

Regulation 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) (2016) OJ L 119/1.

Treaty on the Functioning of the European Union (2012) OJ C 326.

Foreign Jurisdictions

Communications Assistance for Law Enforcement Act 1994 47 USC ss 1001-1002 [United States of America]

Communications (Retention of Data) Act 2011 [Ireland]

Criminal Justice (Terrorist Offences) Act 2005 [Ireland]

Decree on Management, Provision, and Use of Internet Services and Online Information (No 72/2013) [Vietnam]

Foreign Intelligence Surveillance Act 1978 50 USC [United States of America]

TABLE OF ABBREVIATIONS

ANT	Actor Network Theory
CD	Communications Data
CGN	Carrier Grade Network Address Translation
CJEU	Court of Justice of the European Union
CPS	Crown Prosecution Service
CSP	Communication Service Provider
DRI	Digital Rights Ireland
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
GCHQ	Government Communications Headquarters
ICO	Information Commissioner's Office
ICR	Internet Connection Record
ICT	Information Communications Technology
IOCC	Interception of Communications Commissioner
IOCCO	Interception of Communications Commissioner's Office
IP	Internet Protocol
IPC	Investigatory Powers Commissioner
IPCO	Investigatory Powers Commissioner's Office
IPT	Investigatory Powers Tribunal
LEA	Law Enforcement Agency
NCND	Neither Confirm nor Deny
NSA	National Security Agency
OCDA	Office for Communications Data Authorisations
OTT	Over-the-top
UK	United Kingdom
UN	United Nations
UNHCHR	United Nations High Commissioner for Human Rights

INTRODUCTION

In June 2013 a series of disclosures concerning the collection and use of data by the security and intelligence services were revealed by Edward Snowden, an employee of a defence contractor at the United States' National Security Agency (NSA). Amongst these disclosures were revelations that security agencies in both the United States and United Kingdom (UK) had access to the communications records of millions of people.[1] The documents leaked by Snowden showed that monitoring of individuals through their data was occurring on a large scale and was being facilitated by private companies responsible for the collection and generation of that data. Subsequent publications in the press revealed that the NSA was collecting the telephone records and metadata of millions of customers and that the Government Communications Headquarters (GCHQ) in the UK had access to that repository.[2] For his part, Snowden made clear that the decision to disclose the data collection and processing programmes placed society at a crossroads. 'Will the digital age usher in the individual liberation and political freedoms that the Internet is uniquely capable of unleashing? Or will it bring about a system of omnipresent monitoring and control?'.[3]

Regardless of the motives of Edward Snowden and the condemnation from Governments which followed, his disclosures highlighted a worrying trend in the collection and processing of information. Under cover of opaque legal processes, ever increasing quantities of information were potentially being viewed and utilised by State actors.

---

[1] Mirren Gidda, 'Edward Snowden and the NSA files – timeline' *The Guardian* (London, 21 Aug 2013) <https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline> accessed 11 Oct 2014.

[2] Glenn Greenwald, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily', *The Guardian* (6 June 2013) <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> accessed 11 Oct 2014.

[3] Laura Poitras, *Citizenfour* (Praxis Films 2014).

Power dynamics shifted with Governments increasingly being able to know more and more about citizens but with the citizens knowing less and less about how they were being monitored by the government. Conversations which had previously been confined to privacy advocates and civil liberties groups were brought to the fore of public consciousness. Mass surveillance became a common term in public discourse. Glenn Greenwald, one of the journalists responsible for publishing the Snowden revelations noted that the reaction to the disclosures 'triggered an intense, sustained worldwide debate precisely because the surveillance poses such a grave threat to democratic governance'.[4] The collection of data, whether it related to criminals or non-criminals raised serious challenges for democracy and fundamental rights.

In this charged political context, two joined cases were pending before the Court of Justice of the European Union (CJEU), *Digital Rights Ireland v Minister for Communications* and *Michael Seitlinger & Ors.* The outcome of these cases would reflect the shifting attitudes towards the collection of information, and particularly its retention for later use by law enforcement, and shape legislative changes across the EU. Key to these cases was the impact the data retention processes had on the rights to private, family, and home life. The ruling in the joined cases would serve to invalidate the data retention policies across the EU, triggering a wave of legislative changes. In the United Kingdom, such changes found form first in the Data Retention and Investigatory Powers Act 2014 and subsequently in the Investigatory Powers Act 2016. These Acts provide legislative underpinning to the collection, retention, and processing of data which is utilised by public authorities.

[4] Glenn Greenwald, *No Place to Hide* (Penguin 2014).

Yet these Acts do not address the threats to democratic governance posed by the increasing use of surveillance technologies to monitor *en masse*. The technology provided for under these Acts serves as a tool for retaining more data, for enabling ease of access to that data, and for enhancing the analytical capabilities which can be applied to the data. Rather than enshrine the fundamental rights principles key to a democratic society, the Acts further intrude on individual liberties. Law enforcement powers are increased, as are the obligations placed upon private actors to facilitate these powers. Surveillance is conducted by a wide variety of actors utilising technologies which were not originally designed for the purposes of surveillance, thereby creating a surveillant assemblage.[5] This assemblage is utilised to promote State interests that result in limitations on civil liberties, and notably for the purposes of this thesis, privacy. The powers conveyed by these Acts are dynamic and frequently changing. As such, the thesis engages with a highly topical area of law and aims to address the developments in technology and law which violate privacy in this context. In so doing, the thesis aims to fulfil a gap in the literature by assessing privacy in the particular context of the investigatory powers instruments in the United Kingdom and argues that these instruments fail to adequately consider the normative changes which have resulted from the development of these powers. The thesis therefore argues that the collection and use of communications data for law enforcement purposes results in a disproportionate encroachment on privacy.

[5] Judith Rauhofer, 'Privacy and Surveillance: Legal and Socioeconomic Aspects of State Intrusion into Electronic Communications' in Edwards and Waelde (eds), *Law and the Internet* (Hart Publishing 2009) 571.

I. The Focus of the Analysis: Communications Data

The focus of this thesis will be on the retention and processing of communications data. Communications data concerns the who, where, when and how of a communication but, crucially, omits the what. In this way it is distinct from 'content data' which concerns what is being said or written. Communications data was chosen as the focus of the thesis for several reasons. Principally, it is a key tool for law enforcement in the investigation and detection of crime. Indeed, at times the examination of communications data may be the only avenue for investigation. As the former independent reviewer of terrorism legislation David Anderson QC recognised:

> Some categories of crime, such as online crime, could not be investigated without [communications data]. In these cases, they also provide an opportunity for law enforcement to be proactive, looking for suspects rather than waiting until a crime has been committed and a complaint made.[6]

Yet safeguards and oversight for this type of data are considerably weaker than its content counterpart. Communications data is not subject to the warrant requirements that govern the interception of content. Nor are authorisations to access this type of data subject to judicial approval; a designated person within the law enforcement agency may authorise the request. Knowing that communications data can disclose the information necessary but without the stringent processes required for access to content data results in the data being relied upon in an increasing number of areas. This is clearly evidenced through the prevalent use of the data by public authorities generally. In 2016, 754,559

[6] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (Stationary Office 2015) 7.47.

items of communications data were acquired by public authorities.[7] Of that 93% of the data was accessed by police and law enforcement agencies.[8] As communications data becomes more widely used in investigations, it reinforces its value to police as an effective tool. As Elkin-Koren and Haber recognise, this creates a feedback loop, wherein 'as governments become more dependent on data generated … for governance and law enforcement purposes, they develop a stake in facilitating more collection of data'.[9] This results in more categories of data being classed as communications data in the relevant Acts, thereby expanding the data pool on which the police can rely.

Furthermore, communications data is not subject to the same admissibility limitations as its content counterpart. Where the contents of communications are intercepted, the material is not admissible as evidence in the British criminal courts. Under RIPA, disclosure to the defence of intercepted communications is precluded.[10] Such a prohibition does not contravene the principles of a right to fair trial as both parties are prevented from relying on the intercept material in court.[11] As a consequence, the interception of communications is seen as an investigatory mechanism; an information gathering tool rather than an evidentiary tool. Communications data is both. It may provide valuable leads or information relevant to an investigation and, significantly, it is

[7] Stanley Burnton, *Report of the Interception of Communications Commissioner* (2016, HC 297). This figure represents a 42% increase in access since statistical information has been provided for this type of information. In the first IOCCO report to provide the statistical information concerning requests for this data (2005) 439,054 items were acquired. Since then, there has been a year on year increase in the amount of data acquired.
[8] *Ibid*
[9] Niva Elkin-Koren and Eldar Haber, 'Governance by Proxy: Cyber Challenges to Civil Liberties' (2016) 82 Brooklyn L R 105, 144.
[10]Regulation of Investigatory Powers Act 2000 s 17. However, there are some instances in which this material can be disclosed, namely for prosecuting offences under RIPA itself, such as unlawful interception. The material may also be disclosed in proceedings before the Investigatory Powers Tribunal.
[11] Oxford Pro Bono Publico, 'Legal Opinion on Intercept Communications' (University of Oxford 2006); *Jasper v United Kingdom* App no 28901/95 (ECtHR, 16 Feb 2000) held that the bar on disclosure of intercept evidence was consistent with Article 6 ECHR.

admissible and used extensively as evidence in court.[12] Even following judicial rulings which invalidated the policies by which the data was retained, the evidence gathered through those retention processes remained admissible in legal proceedings.[13] Coupled with the lower requirements for access, this increases its value in the overall criminal justice process.

The nature of communications data and the frequency with which it is utilised by law enforcement indicate its importance to the investigation, detection, and prevention of crime. As communicative technologies advance, particularly those which occur online, this data is more readily and consistently available. Legal developments demonstrate a tendency towards classifying more types of data as communications data. The impact of these developments has made it possible for individuals to be knowable without law enforcement having access to the content of communications. The thesis aims to fill a gap in the literature by assessing the nature and impact of technological and legal developments on communications data and how they have impacted on the powers of law enforcement.

II. The System at Issue: Information Communications Technology

The significance of communications data is best evidenced through a discussion of the Information Communications Technology (ICT) system through which it is generated. Crucial to this are the social, technological, and political factors which have motivated

[12] Jon Murphy, National Co-ordinator for Serious and Organised Crime for the Association of Chief Police Officers stated: 'The access to communications data is a fundamental investigative capability which is used daily by police officers to investigate 'serious crime' and save lives, as well as being used routinely as a core element of the prosecution evidence in court'. Home Office, *Protecting the Public in a Changing Communications Environment* (Cmd 5668, 2009) 26.

[13] European Union Agency for Fundamental Rights, *Fundamental Rights Report* (FRA 2016) 125.See also the cases of *DPP v Graham Dwyer* (2014) CCCD [Ireland] and Estonia Criminal Chamber of the Supreme Court judgment no 3-11-1-51-14 23 Feb 2015 [available: https://rikos.rik.ee/LahendiOtsingEriVaade?asjaNr=3-1-1-51-14].

the development of this system and resulted in more categories of data being collected and processed. 'Individual habits, perceptions, concepts of self, ideas of space and time, social relationships, and moral and political boundaries have all been powerfully restructured in the course of modern technological development'.[14]

Law enforcement agencies[15] are dominant end users of ICTs. Whilst these technologies and associated interception and processing methods are not necessarily created for pursuing criminal justice objectives,[16] they serve an effective role in the investigation, detection, and prosecution of crime. Technologies are significantly advancing from their forebears in the nature of data, the scale and scope of operations, the elimination of temporal limitations, the removal of traditional boundaries, and the deconstruction of the individual into discrete 'data'. Developments have increased storage capacities, transmission speeds, and allowed for better analytical processes through aggregation and automated processing. The increased saturation levels of technology in society have made this data more extensive and accordingly more valuable. Law enforcement agencies have capitalised on these developments, leading to new methods of monitoring and tracking, complemented by permissive access rules and analytical techniques.

Despite the role of law enforcement in the eventual use of these technologies, the creators and controllers of these technologies are private actors. In the context of ICT systems, providers of communications services are identified as the control and access points for the necessary information. As a result, these entities are a principal focus of the

[14] Langdon Winner, *The Whale and the Reactor* (U of Chicago Press Books 1986) 9.
[15] For the purposes of this thesis, law enforcement agencies refers to the territorial police services, national law enforcement agencies (including the National Crime Agency), and other police services who have specific remits (such as ports and harbour police forces).
[16] In fact, most technologies are created for commercial purposes and then co-opted by these agencies. Bruce Schneier [*Data and Goliath* (WW Norton & Co 2015) Loc 759] notes that the data collection and processing procedures used by businesses are in effect surveillance models, and these products are optimised when individuals have less privacy.

investigatory powers laws governing the ultimate use of communications data. A striking feature of the current law enforcement strategy in the United Kingdom is the extent of the obligations on these providers, as private actors, to enable and complement law enforcement objectives. Rather than merely operating databases of information which are left to law enforcement to utilise and interpret, private actors are increasingly being asked to perform functions relating to the investigations themselves, such as applying filters to information to seek out potential suspects and witnesses. The private actors are under a mandatory obligation to comply.[17] Such a system effectively imposes the role and duties of a public authority on a private company. These companies must then act as intermediaries, operating enforcement mechanisms via the network infrastructure, without being subject to the obligations placed on public authorities under the human rights instruments. Private actors operating in this manner are under no responsibility to do so in a transparent manner; the methods and processes through which they collect and utilise data under these instruments are not subject to public scrutiny. The lack of transparency surrounding the proceedings renders it difficult to hold these actors to account for their role and the subsequent consequences of their actions in performing these duties. As such, there is a lack in the protections afforded to individuals whose data is collected and processed.

The relationship between the public and private is crucial to understanding the social, political, and technological factors which exist within the ICT system. Changes in technology may usher in changes in social and political norms and similarly changes in those norms may alter technologies. The two are interrelated and must be treated as such in analysing the impact of these developments. Therefore, this thesis focuses on the co-

[17] Potential actions for non-compliance include civil proceedings being brought by the Secretary of State for an injunction or for performance of a statutory duty under the Court of Session Act 1988 s 45; see Investigatory Powers Act 2016 s 95(5).

constructed relationship between privacy, and its underpinning social, political, and technological factors, and information communications technologies. The focus herein is on assessing the role of privacy in the context of investigatory powers mechanisms which govern communications data used by law enforcement agencies. It is in this context that privacy must be assessed in order to determine what interferences have resulted and novel ways that privacy may be under threat. Such an assessment is necessary to subsequently prescribe changes to these mechanisms which can better protect this right.

III. Conceptualising Privacy

The context is particularly important to the concept of privacy here as the thesis approaches privacy as a context relative concept. Technology and privacy have evolved alongside each other, with conceptions of what privacy embraces being responsive to contemporary social and political developments. As observed by Solove, 'The history of communications privacy indicates that it was more the product of social desires than existing realities'.[18] Communications were considered private not because the technologies inherently made them so, but rather because people wanted them to be viewed as such. The role of society in shaping what is deemed private is therefore crucial. It is necessary to look not only at how privacy of communications is viewed in the past and present, but also examine how it should be viewed in the future. 'Privacy is a condition we create, and as such, it is dynamic and changing'.[19] A key question for this thesis is what society is looking to protect when it discusses privacy in the context of

[18] Daniel Solove, *Understanding Privacy* (Harvard University Press 2008) 62; for further discussions on the historical relationship between privacy expectations and communications systems see David Siepp, *The Right to Privacy in American History* (Harvard University Program on Information Resources Policy 1978) 11: 'Nineteenth century public opinion regarded the 'sanctity of the mails' as absolute in the same way it esteemed the inviolability of the home'; Claude Fisher, *America Calling: A Social History of the Telephone from 1940* (University of California Press 1994) 71: 'from the beginning of telephony, people expressed concern that they were being overheard, at first simply by others in the same room – one had to speak loudly – and then by operators or fellow subscribers on a party line'.

[19] Solove n (18) 65.

technological developments in the field of communications. Developments in the ICT system threaten privacy by blurring traditional spatial distinctions, whilst the automatic, all encompassing, and ubiquitous nature of communications systems have increased privacy's collective value.

In assessing the privacy intrusions which result from these technologies, it is necessary to determine what is meant by the term privacy. There is no singular definition of privacy. Conceptualisations take several forms. Privacy may be seen as a right which must be balanced against other values or as a critical constitutive element of values and universal principles. Theorists utilising these conceptualisations attempt to isolate a common denominator of privacy in order to determine its value. These concepts focus on distinct commonalities in purposes or ends such as: the right to be let alone to protect ones thoughts and a sphere for self-development;[20] the right to limit access to the self;[21] the ability to control personal information;[22] and secrecy.[23] Similarly, these concepts focus on utilising privacy to enhance and develop other rights by defining privacy as a right integral to the individual.[24] However, these conceptions are insufficient for the analysis

[20] This concept is rooted in Warren and Brandeis's seminal article 'The Right to Privacy'. The authors establish that man has more than a mere interest in property; rather his thoughts and creations from an integral part of the 'self' and should be protected from appropriation by others; Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890-1891) 4 Harv L Rev 193.

[21] Proponents of this concept argue that man should be entitled to remain apart from others and free from unwarranted access in order to further self-development. This is established by theorists such as Hyman Gross, 'The Concept of Privacy' 1967 NYU L Rev 34 and Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (Pantheon 1983) 10-11.

[22] Theorists such as Alan Westin [Westin, *Privacy and Freedom* (The Bodley Head 1967)] and Charles Fried [Fried, 'Privacy' (1967-1968) Yale L J 475] noting that privacy violations result when information about us is communicated to others without the permission of the subject.

[23] Conceptions of secrecy equate the desire for privacy with having something to hide. Advocates of this conception, such as Richard Posner [*The Economics of Justice* (Harvard University Press 1981) 272] believe that actors require privacy to conceal facts about themselves, and privacy is violated when these facts are disclosed. According to Posner and others, privacy as a means to promote secrecy is inherently contrary to the overall social welfare and is equated with deceptive purposes.

[24] Conceptualisations which emphasise the importance of privacy to the individual often find its value in promoting two distinct concepts: personhood and intimacy. Notions of personhood find value in privacy in enabling the protection of the integrity of the personality; in creating the elements that allow a person to become an individual [Jed Rubenfeld, 'The Right of Privacy' (1988-1990) 102 Harv L Rev 737]. These elements include choices such as who to marry and what to do with one's own body. Conceptions of intimacy draw privacy's value from the benefits it provides to human relationships [Fried n(22) 475].

of privacy intrusions resulting from information collection and processing mechanisms. Privacy intrusions resulting from collection and processing cannot be clearly categorised into any of the preceding concepts; rather, they possess elements relevant to each. Whether an individual will see an action as an infringement of privacy will depend on the context in which it occurred. For example, the privacy interests at issue in the thesis do not merely relate to the fact that information is accessed; rather, the concern is when someone accesses or uses that information in a way which does not conform to expected informational norms. Further, technical capabilities mean that spatial boundaries may not be violated in the traditional sense; the State no longer must physically intrude into a space in order to obtain the desired information. However, this does not mean that a privacy violation has not occurred.

In contrast to the preceding approaches which attempt to identify a common value to the myriad interests privacy protects, the thesis takes an approach based on Wittgenstein's idea of 'family resemblances' which provides for the interpretation that privacy is composed of numerous distinct yet interrelated things.[25] The value of privacy will be dependent on the particular context in which it is engaged.[26] In order to conceptualise privacy as it relates to communications technologies, this thesis employs Helen Nissenbaum's approach of contextual integrity. 'Contextual integrity functions as a framework that is sensitive to meaningful changes affecting people's reactions to new systems or practices'.[27] Nissenbaum's approach allows for an analysis of how

[25] Ludwig Wittgenstein, *Philosophical Investigations* (Blackwell Publishers 2001) ss 66.
[26] Examining privacy in context is supported by many theorists, among them: Robert Post 'The Social Foundations of Privacy: Community and Self in Common Law Tort' (1989) 77 Cal L R 980 who states that information can only be determined to be private when we 'have some notion of the circumstances surrounding the revelation of that information'. Serge Gutwirth [*Privacy and the Information* Age (Raf Casert 2002) 34.] defines privacy by its context and relations to society. Gary Marx ['Murky Conceptual Waters: The Public and the Private' (2001) 3 Ethics & Info Tech 157] argues that the public and private are fluid and dependent on the particular situation or context.
[27] Helen Nissenbaum, *Privacy in Context* (Stanford University Press 2010) 190.

technology shapes expectations of privacy in a manner which accounts for contexts, roles, norms, and values. Her framework argues that 'technologies, systems, and practices that disturb our sense of privacy are those that have resulted in *inappropriate* flows of personal information. Inappropriate information flows are those that violate context-specific informational norms, a subclass of general norms governing respective social contexts'.[28] When there is a violation of these context-relative informational norms, there is a *prima facie* privacy violation and the question becomes whether the changes effected by the norms are justifiable in moral and political terms. The contextual integrity approach does not merely assess how technical systems function, but determines how they relate to social structures as well. It is therefore a useful basis on which to frame an analysis of information communications technologies.

IV. The projects central questions

The core question addressed by this thesis is how, and to what extent, do the current legal and policy frameworks governing the retention of, access to, and analysis of communications data by law enforcement, constitute a violation of privacy which requires substantive changes to the legal regime?

This core question is supported by several supplemental questions.

- How are information communications technology methods and processes organised and utilised to pursue criminal justice objectives?

[28]Helen Nissenbaum, 'Respect for Context as a benchmark for privacy online: what it is and isn't' 286 in Roessler and Mokrosinska (eds) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015) 360.

- How and to what extent is the development of the information communications technology reflective of a co-constructed relationship between law and technology?
- How and to what extent are these technologies regulated and deployed in a manner that accommodates privacy values?
- What is meant by privacy in the context of communications data?
- Can conceptions of privacy rooted in traditional liberal values be maintained or must privacy be re-conceptualised to accommodate the role of technology?
- How do ICT processes utilised and deployed by law enforcement affect this defined privacy right?
- How can the laws and policies in this area be developed in a manner that strikes an appropriate balance between privacy rights and the criminal law enforcement objectives of the State?

These questions, once answered, will address the key aim of this thesis, namely prescribing an alternative legal regime for communications data which protects privacy. By addressing the topic on this level, it is believed that the thesis will open a line of research to other areas where the police use non-typical categories of data in their investigations. As new types of data are generated which no longer clearly fit into the pre-existing boxes of 'content' or 'communications' it is necessary to determine a different way to treat that data so fundamental rights of privacy can remain protected.

V. Methodology

This thesis takes an interdisciplinary approach, combining law, technology, and sociology. The communications technologies are examined in the context[29] of the ends they serve for law enforcement and national security. Yet, 'communicative technologies sit slightly awkwardly with the other applications [of the technology] since they have no claim to be specific to crime control and therefore cannot be seen as a purpose or function of criminal justice'.[30] The principal aim of these technologies is to facilitate interactions between individuals and this is accomplished through private means. Communicative technologies do not exist separately as a tool for law enforcement but rather are co-opted in to the policing process. It is therefore difficult to analyse and regulate these technologies using traditional criminal justice frameworks. Thus, it is instructive to use an alternative framework which does not simply look at the ultimate end use of these technologies by law enforcement but at other social and technological factors which contribute to the value of these instruments. This relationship between law enforcement and ICT lends itself to a systems theory framework.

This framework acknowledges that law and technology are complex and interrelated structures which shape and define each other. In terms of communications technologies, an analysis cannot be separated from the social context nor from the way the technology has come to shape society. The value of the information derived from the ICT system comes from the nature of the data generated by the system, which is expansive in its scope and generated on an exponentially increasing scale. As the technologies permeate

[29] Contexts here are defined as structured social settings characterised by roles, relationships, power structures, norms, and values. [Nissenbaum n(27) 132]

[30] Ben Bowling Amber Marks and Cian Murphy, 'Crime Control Technologies: Towards an Analytical Framework and Research Agenda' 60 in Brownsword and Yeung (eds), *Regulating Technologies* (Hart Publishing 2008).

everyday life, their impact on society increases. Concurrently, so does their value to law enforcement which requires more advanced technical means to be employed to fully capitalise on this growth of data. These developments reflect on established social norms, including that of privacy. As explained by Beate Roessler,

> Social norms governing informational private *constitute* and *regulate* different social relationships. Insofar as these social relationships, practices, and roles are constitutive for society, so too is the protection of privacy of these relationships and the individuals engaged in them.[31]

A systems theory approach, in line with that developed by Hughes, allows for the fact that there is a mutual or co-constructed process between technology and society.[32]

The systems theory framework acknowledges that technologies cannot be divorced from society; but nor are they purely social constructs.[33] The approach to systems theory utilised in this thesis is based largely on the work of Thomas P Hughes and acknowledges that systems are complex interdependent arrangements of technology, cultural factors, social actors, and situated meanings.[34] All aspects of the system can be interconnected; no greater value is placed on one element over the others. Elements of the system can be classed as physical, organisational or legislative. The system does not develop in a linear fashion but evolves through various phases which overlap and backtrack as the system develops. Through this process of development, the elements of the social are incorporated further into the system, allowing it to be assimilated into

[31] Beate Roessler, 'Privacy and social interaction' (2013) Phil & Social Criticism 779.
[32] Priscilla Regan, 'Privacy and the common good: revisited' 51 in Roessler and Mokrosinska (eds) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015) 360
[33] Torin Monahan, 'Questioning Surveillance and Security' in Johnson and Wetmore (eds), *Technology and Society: Building our Sociotechnical Future* (MIT Press 2008) 545
[34] Regan n(32) 51.

society. However, issues arise within these systems when the components fall out of sync with other elements of the system. In Hughes's systems theory, such elements are known as reverse salients. Further development of the system occurs when reverse salients are identified and the system is altered in some way as a result. The changes made as a result of a reverse salient will be dependent on the actors and contexts which are involved and will be informed by their specific values and goals.

This thesis argues that the ICT system utilised in the collecting and processing of communications data, and governed by investigatory powers legislation, changed traditional norms associated with information in the context of law enforcement. This has been accompanied by changes in legislation which do not reflect the significance of this shift in norms. This thesis argues that instead of taking technological changes into account, the law seeks to apply traditional communication norms which are based on technologies which were limited in their scope, scale, and spatial bounds. Under traditional communications norms, a clear distinction could be made between various types of data. Communications data was 'envelope data'; information that could be easily derived from merely looking at the outside of an envelope and therefore did not benefit from any expectation of privacy. The data generated was that which companies needed in order to provide the service and bill their customers. The information provided went no further. Current legislation still uses these analogies of 'envelope data' and mere 'billing information' to class communications data which is now capable of revealing extensive personal and private information. The law does not acknowledge that the value and intrusiveness of this category of information has changed as a result of the development of technology.

Within Hughes's terminology, the failure of law to account for the changing social norms associated with this information results in a reverse salient which requires correction. However, the size and scope of the ICT system has provided it with technological momentum. As will be discussed further in Chapter 2, such momentum makes the system resistant to change. When assessing how the system may be altered to take into account these significant changes, it is necessary to examine the variety of technical elements, modes of communication, legislative aims, and organisational structures which form the system. All of these elements possess their own political, economic, and social motivations. The thesis argues that the elements must be addressed in order to determine how the identified issues within the system can be corrected, with the particular aim of incorporating an effective conceptualisation of privacy.

A. Methods

To identify the relevant relationships and issues between communications data, law enforcement, and privacy, a multi-disciplinary approach is taken which permits the relevant factors from the fields of law, sociology, and technology to be incorporated into the analysis. It is necessary to understand these varied and sometimes competing factors to be able to prescribe effective legal and policy recommendations for the future. The extant legal frameworks are assessed through statutory interpretation and case law analysis at both the domestic and European Union levels. In analysing these primary sources, the accompanying *traveaux preparatoires* and Hansard debates are utilised to provide a wider understanding of the factors which influenced the development of the law. Secondary instruments which are primarily concerned with the implementation of

these primary sources, namely relevant Codes of Practice and Statutory Instruments,[35] are analysed to determine the practical impact and use of the powers set forth in the legislative mechanisms. Where it provides a useful comparator, information regarding the communications data policies of other jurisdictions is discussed. This is particularly evident in the concluding chapter which sets forth prescriptive measures to be taken to amend the investigatory powers instruments to better protect privacy as conceptualised in this thesis. This thesis also draws on secondary scholarship in the area of law, technology, and sociology. The analysis of this literature informs the discussion of what norms and values need to be incorporated into the system in light of the technology. The elucidation of norms and values is critical to understanding privacy as conceptualised herein. Therefore, the focus is on those norms and values which relate directly to the processing and collecting of data and communications. The body of literature engaged with looks at how the various disciplinary fields utilise these concepts. The contours of privacy established through this assessment are then used to unpack the legislative developments and technological practices of the system.

In addition to the critical analysis of primary sources and scholarship, select semi-structured interviews were undertaken. The interviews were approved utilising the ethical approval process set by Kent Law School. These interviews are rooted in a romantic epistemology, the focus of which is on the participants' beliefs, perspectives, opinions, and attitudes concerning the investigatory powers mechanisms and their particular experiences.[36] This allows the emphasis to be placed on 'what the interviewee

[35] Home Office, *Acquisition and Disclosure of Communications Data Code of Practice* (March 2015); Home Office, *Operational Case for the Retention of Internet Connection Records* (4 November 2015); The Investigatory Powers Tribunal Rules 2000, SI 2000/2665.

[36] Kathryn Roulston, 'Considering quality in qualitative interviewing' (2010) 10(2) Qualitative Research 206. For more discussion on the specifics of the romantic approach see: Mats Alvesson, 'Beyond Neopositivists, Romantics, and Localists: A Reflexive Approach to Interviews in Organisational Research' (2005) 28(1) Academy of Management R 13.; David Silverman, *Interpreting Qualitative Data: Methods for Analysing Talk, Text, and Interaction* (Sage 2001)

views as important in explaining and understanding events, patterns, and forms of behaviour'.[37] This interview technique was selected in order to allow conversations to flow freely and let the interview subjects speak about the areas of interest from their own perspective. Whilst these interviews were not the core methodological approach employed in the thesis, they do provide insights which are illustrative of the issues raised by the use of communications data. In approaching interview subjects, three key groups were identified: industry, activists, and public actors. Each group has a different approach to communications data and will stress certain factors over others in the development of the system.

In the area of industry an interview was undertaken with the head of the Internet Service Providers Association. The goal of this interview was to gain an industry perspective on the requirements imposed on these companies and what, if any challenges they perceived with implementing the requirements delegated to them under the legislation. Throughout the interview, technical issues with the processes required of Communication Service Providers (CSPs) became apparent. These issues underpin the critique of the retention, access, and analysis elements of the system discussed in Chapters 3 to 5. With regard to activists, two interviews were undertaken. One concerned the use of communications data relating to journalistic material. The other was a discussion about the investigatory powers instruments more generally. The core focus of each of these interviews was the overall impact on human rights, and in particular, privacy that occurred as a result of the use of these powers. Finally, with regard to public actors, the head of a relevant oversight agency was interviewed. This interview provided a more thorough understanding of the practical capabilities of the oversight agency and its limitations. In

[37] Alan Bryman, *Social Research Methods* (Oxford University Press 2012) 468; Carol Warren, *Handbook of Interview Research* (Sage Publications 2002) 83.

formulating an alternative process for ensuring privacy in the context of communications data, it is necessary to provide for an adequate oversight structure. The interview is used to direct the formation of that structure.

The aim of these interviews was to gain a first-hand understanding of how the relevant actors saw the law and their relationship to it. As individuals engaged with the law and its functioning, the interview subjects were able to bring to light areas which were not apparent from doctrinal research. Direct accounts from these professionals are instructive and are incorporated in to the analysis in subsequent chapters.

In speaking with the head of IPSA, it was made apparent that the industry viewpoint on the use of the communications data powers was largely concerned with functionality and cost effectiveness. The concerns raised in this interview related to implementing the provisions rather than any restrictions or legal requirements necessary to provide the information. This was interesting, particularly as the public dialogue advanced by these CSPs so often discusses the importance of their users and their rights. With regard to the activist interviews, the content largely followed the criticisms and critiques of the law which these bodies publicly advance. Little additional insight was garnered. However, with regard to public authorities, the interview with the acting head of the IOCC offered unique insight into the functioning and limitations of the oversight body. As the audits undertaken by this body were confidential, with only a general report on their outcomes provided to the public, the interview with the head of the IOCC allowed for greater understanding of the functions of that body.

Additional interviews were sought with actors from within the police. The targets of these request were the ‘designated persons’ and ‘single point of contacts’ who deal with approving and processing requests by public authorities for communications data. It was

hoped that by speaking with individuals directly involved in the approval processes, it would be possible to determine the standards and criteria that the public authorities apply before granting access to communications data. As the law requires that these requests be judged against the standards of necessity and proportionality, these first-hand accounts would provide insights into what factors were taken into account and how the demands for access were balanced against individual rights.

However, it was not possible to secure interviews with these subjects. Approaches were made via phone, e-mail, and post. As the applications for this information are confidential, it was not possible to identify the precise persons within each precinct with which to make contact. As a result, the requests were sent to Chief Constables of the police authorities as well as press officers. One of two outcomes resulted from the attempts to make contact: the request, and subsequent follow-up request, would simply go unanswered; or a response would be provided with links to websites containing information on police use of communications data and/or police standards and ethics. Therefore, it was not possible to interview these individuals. The reluctance of public authorities to speak to how these powers are used represents a further limitation of the material available in this area and raises concerns for the transparency of the process as it relates to communications data.

B. Methodological limitations

As noted, this project engages with a very topical area of law. Whilst this has made it an engaging and relevant area to research, it is necessary to acknowledge the limitations of the material. At the time of writing, a consultation has been issued by the Government concerning the Investigatory Powers Act and proposed changes to the regime. Similarly, three cases of note are currently going through the courts and are at various stages. It is

envisaged that the outcome of either/both the consultation and the cases will result in changes being made to the law as it stands. Where possible in subsequent chapters, the potential implications of these changes are discussed. However, it is not possible to confidently foresee any and all potential outcomes at this stage.

VI. Chapter Overview

The thesis begins by defining the conception of privacy against which to assess the interferences which occur through the collection and processing of communications data by law enforcement. In order to conceptualise privacy, Chapter 1 first looks to the existing conceptions rooted in Western liberal thought. Each of these conceptions are evaluated for their perceived benefits and shortcomings in determining how privacy is impacted in the use of communications data. The thesis argues that the established conceptions of privacy cannot adequately address interferences with the right to privacy which arise as a result of the use of this data. As such, an alternative conception of privacy will be applied. This conception is based on Helen Nissenbaum's theory of contextual integrity. Chapter 1 sets out the reasoning behind the selection of this approach. The chapter then proceeds to outline how this definition of privacy will be applied in the context of the ICT system utilised by law enforcement. Determinant factors which dictate the informational norms breached in this context are summarised to provide the foundational elements which will be discussed in assessing how retention, access, and analysis of data affect privacy. The overall aim of this chapter is to provide the foundation for the subsequent evaluation of the impact on privacy of the ICT system.

Following the conceptualisation of privacy in Chapter 1, Chapter 2 will define the parameters of the system which is the context in which that concept is to be applied. Chapter 2 establishes that privacy will be assessed in the context of the information

communications technology system which is ultimately responsible for the collection and processing of communications data. The aim of this chapter is to determine how the ICT system is reflective of a co-constructed relationship between law and technology. In order to evaluate this relationship it is necessary to examine technological and social developments and evaluate the components of the ICT system and the traditional norms associated with these processes. To do so, the thesis utilises Hughes's systems theory approach which is defined in Chapter 2. The selection of systems theory is oriented within the body of extant literature on law and science and technology studies. Hughes's systems theory approach is then applied to the ICT system. The discussion of the development of the ICT system and the elements which comprise it allows for an assessment of the changes in context relative informational norms and an evaluation of how to better guarantee these norms in future developments. The framework created in Chapter 2 will be applied to the specific processes of the system discussed in Chapters 3 to 5.

Chapter 3 examines the first of these processes, namely the collection and retention of communications data. The data retention element is a critical component of the ICT system. It is only through the retention of large amounts of communications data that law enforcement can benefit from subsequent access and analysis capabilities. As such, it is necessary to set forth the precise dictates of the data retention process. In Chapter 3 this is done by first undertaking a thorough examination of the evolution of the data retention system, with reference to technological and legislative developments that underpinned its creation. The current dictates of the data retention policies are then established. The concept of privacy established in the preceding chapters is then examined in light of the powers of retention. Specific attention is paid to the information types, transmission principles, and actors engaged in the retention process. These

elements are assessed to determine the overall impact on context relative informational norms. This analysis argues that there has been a breach of contextual integrity in the retention of the data.

Chapter 4 then goes on to address the second function of the ICT system, namely facilitating access to the retained data. The focus of this chapter is on the manner and mechanisms through which law enforcement officials are able to access communications data. Historic examples of access provisions are compared to the current technological context. External factors to the technological developments are assessed to determine their impact on the evolution of the system. It is established that the existing access provisions indicate that law enforcement can retrieve the information more readily than previously possible. The limitations on access have been altered with the balance shifting toward law enforcement over the individual. The analysis of these changes suggests that there has been a breach of contextual integrity and thereby a violation of privacy.

The final function of the ICT system that is addressed in the thesis is that of analysis which is the subject of Chapter 5. Analysis here means the methods through which greater meaning can be derived from the communications data. This is accomplished through applying additional technological processes to the information to generate data that is more relevant to law enforcement. Principally, with regard to communications data this occurs via three processes: IP address resolution, the 'request filter', and downstream use of the data. The specifics of these processes are addressed in this chapter. It is argued that the analytical techniques employed pose a distinct threat to privacy.

The treatment of retention, access, and analysis in these chapters reveal breaches in contextual integrity which result in privacy violations. The question then becomes how the privacy violations may be offset by oversight and remedial mechanisms designed to ensure that these violations are justified in accordance with the law. Chapter 6 focuses on the current methods which are used to ensure that such privacy violations only occur where they are necessary and proportionate. In doing so, the focus is on the additional safeguards and oversight mechanisms which apply to the collection and processing of the communication data. Chapter 6 offers a thorough critique of the existing powers, examining the key agencies who are involved, namely, the Information Commissioner, the Interception of Communications Commissioner, the Investigatory Powers Commissioner, and the Investigatory Powers Tribunal. The analysis developed herein determines that these mechanisms are insufficient to offer the necessary safeguards for privacy to ensure that the investigatory powers measures are in accordance with the rule of law.

Finally, the thesis will offer Conclusions and Proposals for Reform. In this chapter, the discussion will examine the findings evidenced in the preceding chapters which demonstrate that, through the development of the ICT system, fundamental informational norms have been altered, representing a privacy violation which has not been adequately provided for in the current legal and policy regimes. This chapter then goes on to offer prescriptive policy recommendations to address the shortcomings in the current legal framework. These recommendations are aimed at ensuring that the informational norms inherent in the use of communications data generated by the ICT system protect privacy as conceptualised under the contextual integrity decision heuristic. The practical recommendations propose mechanisms for purpose limitation, data minimisation, an increase in the rights of individuals, and a reclassification of CSPs. These

recommendations will thereby mitigate the privacy intrusions created by the use of technology to collect and process communications data. Such a framework addresses the failings of the current regime and offers mechanisms to ensure that privacy as defined in this thesis can be protected in light of technological developments in communications systems.

CHAPTER 1: CONCEPTUALISING PRIVACY

I. Introduction

This chapter presents the key concepts and literature on privacy and develops a conception of privacy which can accommodate the development of the technological system discussed in the next chapter. This conceptualisation is necessary in order to determine the unique characteristics of privacy; what is intruded upon and what we seek to protect when we invoke privacy. Crucial to this analysis is determining whether privacy retains value in a society where it is so easily forfeited for the convenience that modern technology brings. It is important to identify what precisely is meant by privacy in terms of this analysis. Conceptions of privacy draw from biological, historical, sociological, and legal influences. The matters we consider private are not static; they change according to these influences.[1] Despite the variations on what should be considered private, these interpretations are consistent in maintaining that privacy has value. In order to assess privacy's value in the ICT system, this chapter will be comprised of four parts.

Part I discusses the traditional concepts of privacy that have been employed in literature and transposed into law through judicial interpretation and statute. Part II critiques these conceptions in light of technological developments which have altered the traditional interpretation of privacy. Changes in this area can be broadly classified under four distinct areas: temporal, spatial, saturation, and ephemeral. The technologies referred to for the purposes of this analysis are limited to those ICTs which will be discussed in Chapter 2. In light of the analysis of existing conceptions of privacy, Part III posits that

[1]Daniel Solove, *Understanding Privacy* (Harvard University Press 2008) 50.

privacy and technology can best be conceptualised from a bottom-up approach which focuses on the context in which privacy is employed. This section utilises legal scholar Helen Nissenbaum's theory of contextual integrity as the basis for examining privacy through context. This theory forms the foundation of the conception of privacy used in the thesis. Finally, Part IV sets forth the conception of privacy in the context of the ICT system used for collecting and processing communications data.

This conception is based on shifts in information flows, transmission principles, and actors, changes in which result in a violation of context relative informational norms. Each of these factors is assessed in relation to the context of the ICT system. Particular emphasis is placed on the shift in dominant actors and power structures in information collection and processing from governmental to commercial actors; how norms have changed due to the structure of the technology, and whether that is reflective of a shift from traditional panoptic conceptions which often govern issues of monitoring and tracking; and finally whether the values embodied by these technologies are indicative of a shift in the criminal justice system toward more community driven rights. This section argues that changes in the ICT system alter traditional information flows and result in privacy intrusions. The conception of privacy defined in this chapter is then applied to the components of the ICT system in Chapters 3 to 5. Utilising the conception of privacy established in this chapter, the subsequent chapters will argue that processing and collection of data under the investigatory powers mechanisms results in privacy violations which are not adequately protected by the current oversight regime. Through applying a context relative conception of privacy, the impact of the technology can be adequately assessed with the aim of offering effective recommendations for reform.

II. Traditional Concepts of Privacy

Concepts of privacy offer an abstract picture of what identifies privacy in its various manifestations. Despite extensive analysis and debate there is no agreed upon conception of what privacy is, nor what specific elements are required for there to be a violation of privacy. Scholars have argued for a variety of different approaches, alternatively viewing privacy as a derivative right[2] or a constitutive right;[3] attempting to identify a common set of necessary and sufficient elements that exemplify privacy and its 'core' characteristics;[4] or arguing that privacy reflects a plurality of values.[5] The following analysis will look at the dominant concepts of privacy that have permeated the literature before critiquing their effectiveness in determining privacy violations as a result of technology.

a. Spatial

Privacy in its earliest iterations was tied to the notions of space, derived from the idea that there are distinct public and private spheres and an intrusion into the latter represented a violation. American jurists Samuel Warren and Louis Brandeis gave voice to this idea in their article *The Right to Privacy* in 1890. Responsive to technological developments of the time, specifically the development of portable cameras which allowed for the advancement of so-called 'yellow journalism' and a press which could

[2] See: Judith Thomson, 'The Right to Privacy' (1975) 4 Phil & Pub Affairs 295; HJ McClosky, 'Privacy and the Right to Privacy' (1980) 55 Philosophy 37; Harry Kalven, 'Privacy in Tort Law – Were Warren and Brandeis Wrong?' (1966) 31 Law & Contemp Prob 326, 327.
[3] Raymond Wacks, *Law. Morality and the Private Domain* (Columbia University Press 2000) 356.
[4] See: Julie C Inness, *Privacy, Intimacy, and Isolation* (Oxford University Press 1996); David M O'Brien, *Privacy, Law and Public Policy* (Praeger 1979); Edward Bloustein, 'Privacy as an aspect of Human Dignity: An Answer to Dean Prosser'(1964) 39 NYU L R 962; Charles Fried, 'Privacy' (1967-1968) 77 Yale L J 475; Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89 Yale L J 421.
[5] Solove n(1); John Dewey, *Logic: The Theory of Inquiry* (Holt Reinhart and Winston 1938).

record and photograph personal acts like never before, Warren and Brandeis argued for a right to privacy, akin to the 'right to be let alone' to protect the private sphere from intrusion.[6] This privacy right required definitive boundaries between the public and private sphere, wherein the private could not be interfered with. Sociologist Ernest Van Den Haag built upon this idea in his conception of privacy as the exclusive right of an individual to a realm of his own, where others are excluded from watching, utilising, or intruding on his private space.[7] Spatial intrusion remains a common theme in privacy discourse. The intrusions can take a variety of forms, from those associated with infringement of concrete spaces[8] to those associated with more abstract violations such as intrusions that result from noise or odours.[9] The common theme to these interpretations is the idea that there is a spatial element which remains distinct from the public; a space wherein the individual can have a reasonable expectation that they will be safe from interference.

These conceptions rely on the idea that there can be no privacy in public. A conception of privacy based on a delineation of public and private spheres does not account for the idea that there may be an expectation of privacy in a public area. There is discourse on both sides of the issue. Proponents argue that there can be no expectation of privacy once one enters the public sphere whereas others argue that entrance into the public arena does not in itself negate privacy interests.[10] The latter interpretation is reflective of the challenges of the spatial concept of privacy. These difficulties are compounded when

[6] Samuel Warren & Louis Brandeis, 'The Right to Privacy' (1890-1891) 4 Harv L Rev 193.
[7] Ernest Van den Haag, 'On Privacy' in Pennock and Chapman (eds) *Nomos XIII: Privacy* (1971).
[8] Thomas Scanlon, 'Thomson on Privacy' (1975) 4 Phil & Pub Affairs 315, 322.
[9] Richard Parker, 'A Definition of Privacy' (1974) 27 Rutgers L R 280.
[10] This was demonstrated by the ECHR in the case of *Peck v United Kingdom* App no 44647/98 (ECtHR 28 Jan 2003), wherein the court held that although the applicant was in public, he 'was not therefore the purposes of participating in any public event and he was not a public figure' and therefore was entitled to privacy, even though he was in the public sphere.

this conception of privacy is examined in reference to information technology systems. Information cannot be constrained by traditional spatial bounds; it is not always possible to delineate between public and private arenas, particularly in the online sphere. Traditional spatial distinctions are ill equipped to deal with these issues.

Spatial notions of privacy are tied to other conceptions. Professor Randall P Benzanson noted the importance of the notion of a distinctive private space for the development of the individual.[11] This interpretation of privacy as necessary to protect a space for self-development is echoed in further conceptions of privacy, albeit ones that identify the core value of the right, not in the protection of a concrete space, but in the value it has to the individual.

b. Autonomy/Self

This conception of privacy maintains that privacy has value because it promotes the development of the self and individual autonomy. Autonomy conceptions are rooted in liberal ideals of individualism, exemplified by John Stuart Mill in *On Liberty.* Mill argues against the tyranny of the majority, which, by imposing prevailing social opinions and feelings, fetters the development and formation of the individual.[12] Defining privacy in relation to the value it provides for the individual exemplifies the liberal interpretations which underpin much privacy discourse.[13] Individuals are recognised as the key benefactors of privacy[14] whose interest in self-development supersedes community interests in all but the most extreme of cases. As legal scholar Charles Fried puts it,

[11] Randall P Benzanson, 'The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990' 80 Cal L R 5 1133, 1142-43.
[12] John Stuart Mill, *On Liberty* (Andrews UK Ltd 1890) 4.
[13] Beate Roessler: 'In liberal societies, privacy has the function of permitting and protecting an autonomous life.' in Roessler *The Value of Privacy* (Polity Press 2004) 288.
[14] Ruth Gavison notes that privacy 'locates its value in its functional relationship to valued ends, including human well-being and development, creativity, autonomy, mental health and liberty.' [Gavison n(4) 421].

privacy is one of the 'basic rights in persons, rights to which all are equally entitled, by virtue of their status as persons ... it requires recognition of persons as ends, and forbids the overriding of their most fundamental interests for the purpose of maximising the happiness or welfare of all'.[15]

Various theorists have advocated for the importance of privacy as a tool for individual development. Helen Nissenbaum posits that autonomy allows individuals to determine their own principles and subject those principles to review.[16] Moral autonomy, argues Professor Julie Cohen, allows for 'independence of critical faculty and imperviousness from influence'.[17] Privacy is significant in that it allows individuals freedom to think for themselves and develop their own personality without fear of social reprobation which could occur if they were forced to make their views, hobbies, and ideas public. It allows for the development of what American Jurist Paul Freund calls 'those attributes of an individual which are irreducible in his selfhood'.[18] Where there are intrusions on privacy, the conduct often amounts to conduct that is 'demeaning to individuality' or 'an assault on human personality'.[19]

If privacy is necessary for self-development,[20] then technology which interferes with privacy can alter this development. Technology which makes possible the monitoring

[15] Fried n(4) 485.
[16] Helen Nissenbaum, *Privacy in Context* (Stanford University Press 2010) 82.
[17] Julie Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (1999) 52 Stan L R 1373.
[18] Freund created a conception of privacy known as 'personhood' based on this central tenet. Later scholars in the personhood field focus on the role that privacy plays in decisions crucial to the self, such as those concerning abortion, contraception, and marriage; decisions where the state should not interfere. For further discussion see: Paul Freund, 'Privacy: One Concept or Many' in Pennock & Chapman (eds) *Nomos XIII: Privacy* (1971) 182, 195; J Braxton Craven, 'Personhood: The Right to be Let Alone' (1976) 15 Duke L J 699, 702; Bloustein n(4) 962.
[19] Bloustein *ibid* 991.
[20] See Jeffrey Reiman, 'Privacy, Intimacy, and Personhood' (1976) 6(1) Phil & Pub Affairs 26, 39: 'privacy is necessary for the creation of *selves* out of human beings, since a self is at least in part a human being who regards his existence – his thoughts, his body, his actions – as his own'.

and tracking of communications presents distinct risks to personal autonomy facilitated by privacy because it creates a perception of continual observation. Political philosopher Stanley Benn noted the impact of observation on individuals, finding that observation denied individuals respect for persons as choosers 'because they transform the actual conditions in which the person chooses and acts, and thus makes it impossible for him to act in the way he set out to act, or to choose in the way he thinks he is choosing'.[21] There are extrinsic losses of freedom which occur when people curtail outward behaviours due to their unusual or unconventional nature which may have negative consequences.[22] Similarly, there are often intrinsic losses of freedom which occur via self-censorship when individuals realise that their actions might be noted or recorded.[23] Privacy as a facilitator of self-development is frustrated by the technological developments which increase visibility. However, that does not mean that privacy cannot exist but rather that a conception must incorporate this development.

c. Relationships

The idea that privacy enables self-development and autonomy is linked to conceptions which value privacy for its role in building relationships and intimacy. The self cannot develop in a vacuum; interactions with others are a key element of personal growth. Sociologist Arnold Simmel argues that 'we become what we are not only by establishing boundaries around ourselves but also by a periodic opening of these boundaries to nourishment, to learning and intimacy'.[24] Charles Fried similarly advocates for the

[21] *Ibid* 37.
[22] Jeffrey Reiman, 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future' (1995) 11 (1) Santa Clara Comp & High Tech L J 42. This can clearly be seen in instances such as those where people are fired for postings on Facebook or even fail to be hired due to their social media activities.
[23] *Ibid* 44.
[24] Arnold Simmel, 'Privacy is not an Isolated Freedom' in Pennock and Chapman (eds) *Nomos XIII* (1971) 23.

interpretation of privacy as a valuable good due to its ability to foster respect, love, friendship and trust. In fact, Fried argues that, 'Privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable'.[25] Privacy interests are not merely found in personal data and information. They are not bound to secrecy or the prevention of disclosure. Rather, an interest in privacy is related to selective disclosure,[26] allowing individuals to determine who knows what about them, and to utilise that information to develop relationships and nurture intimacy.

Privacy's value in this instance is that it allows individuals to determine what information they share and whom they share it with.[27] How people choose to share information will depend on the context of the relationship.[28] This conception of privacy recognises that individuals do not have a single definitive persona that they present to the world. Different relationships require different behaviours.[29] Privacy allows individuals to be responsive to various contexts and behave in an appropriate manner.

Technology has a direct impact on the ability of individuals to determine the appropriate persona for each interaction. Widespread information creation and dissemination due to the increased production of data occurring through everyday transactions and interactions has made individuals infinitely more knowable. This has a direct impact on ideas of selective disclosure. Indeed, Facebook founder Mark Zuckerberg has criticised this idea.

---

[25] Fried n(4) 478.
[26] Kenneth Karst, 'The Files: Legal Controls over the Accuracy and Accessibility of Stored Personal Data' (1966) 31 Law & Contemp Prob 342, 344.
[27] James Rachels, 'Why Privacy is Important' (1975) 4(4) Phil & Pub Affairs 323, 329; Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Vintage Books 2000) 282.
[28] Ferdinand Schoeman, 'Privacy: Philosophical Dimensions of the Literature' in Schoeman (ed) *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press 1984) 403.
[29] Bruce Schneier, *Data and Goliath* (WW Norton & Co 2015) loc 1931 recognises that we are not the same to everyone we meet and we alter our behaviours accordingly to the situation.

'You have one identity. The days of you having a different image for your work friends or co-workers and for the other people you know are probably coming to an end pretty quickly. Having two identities for yourself is an example of a lack of integrity'.[30] While this is a rather stark depiction, the increase in information as a direct result of technological developments has changed the traditional norms ascribed to privacy which grant the individual control over her various social identities and allow her to formulate her relationships accordingly.

d. Access

In a related conception, privacy is the ability of the individual to limit or deny access to others, in order to protect their own autonomous sphere for self-development. Relatedly, this idea of access was cited by legal scholar Ruth Gavison as a key element of privacy, 'Our interest in privacy,..., is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention'.[31] Crucial to this conception is the idea that the individual exercises control over the access. It is not enough that information remains hidden, but that those to whom it relates are able to control who ultimately has access to the information. The access in this conception is limited in its scope. Hyman Gross stressed this element of limitation, stating that 'privacy is the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited'.[32] This was supported by David M. O'Brien in his book *Privacy, Law, and Public Policy* wherein he found that privacy

[30] David Kirkpatrick, *The Facebook Effect: The Real inside Story of Mark Zuckerberg and the World's Fastest Growing Company* (Virgin Books 2011) 384.
[31] Gavison n(4) 423.
[32] Hyman Gross, 'The Concept of Privacy' (1967) 42 NYU L Rev 34, 36.

'may be understood as fundamentally denoting an existential condition of limited access to an individual's life experiences and engagements'.[33]

Privacy will be diminished not only where access is violated, but also where, even with permission, that access is extensive in reach. This conception of privacy requires the individual to limit information known, an idea that is diametrically opposed to technologies which function most effectively through the constant production of data. However, it is not that the individual's use of technology demonstrates an absolute refutation of the concept of privacy as a limited access conception; rather the practical use of technology enables individuals to share certain information with certain people and not others. When law enforcement agencies access information, even where such information is freely shared with friends or colleagues, it can be said that there is a privacy intrusion.

e. Control

Following on from the view that privacy is rooted in the concept of limited access, is the view that privacy has value because it allows the individual control over information about oneself. This is an expanded view of the preceding concept. Legal scholar Alan Westin defined privacy as 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others'.[34] In a similar vein, E.L. Godkin argued that 'Nothing is better worthy of legal protection than private life, or in other words, the right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the

[33] O'Brien n(4) 262.
[34] Alan Westin, *Privacy and Freedom* (The Bodley Head 1967).

subject of public observation and discussion'.[35] This view is supported by sociologist Edward Shils. 'We say that privacy exists where the persons whose actions engender or become the objects of information retain possession of that information, and any flow outward of that information from the persons to whom it refers (and who share it where more than one person is involved) occurs on the initiative of the possessors'.[36] Unlike the limited access conception, the sharing of information or permitting others access does not diminish privacy. Rather privacy is ensured by granting the individual control over information about themselves.[37] If that information is divulged without the consent of the individual, then privacy is breached, regardless of what the information is. Additionally, privacy scholar Daniel Solove stresses that consent is not the only aspect of control; the individual must be able to ensure that personal information is used for the purposes he or she desires.[38]

New technologies facilitate sharing of information and provide individuals with a method of doing so, thereby allowing them to determine what is shared and providing an element of control. However, where the laws, such as those at issue, remove the element of control over the information through the creation of repositories of data, the disclosure of which the individual has no control over, then there is a concomitant privacy intrusion.

f. Social

The preceding concepts of privacy place its importance in the individual interests and rights it protects, the most significant of which are the freedom and autonomy of individuals, whether as ends in themselves to promote self-development, or as elements

[35] Solove n(1) 19.
[36] Edward Shils, 'Privacy: Its Constitution and Vicissitudes' (1966) 31 L & Contemp Problems 281, 282.
[37] A Michael Froomkin, 'The Death of Privacy?' (2000) 52 Stanford L R 1462; Anita Allen, *Uneasy Access* (Rowman & Littlefield 1998).
[38] Solove n(1) 23-4.

exercised through practices of limited access or control. These individual freedoms are rooted in fundamental liberal democratic societies. However, emphasising privacy's role in protecting the individual is a weak method for protecting privacy in practice, particularly where privacy interests interfere with broader societal interests such as preventing or detecting crime or ensuring national security. Indeed, intrusions with privacy are normally justified on the grounds that such an interference is necessary to protect the community as a whole, and intrusions facilitated by ICT are no different. Yet privacy does not only promote individual freedoms and autonomy; it has a broader social value as well.

Tied in to the social conception of privacy are those conceptions that equate privacy with secrecy. In this concept, privacy is seen as socially detrimental. It is 'a plea for the right to misrepresent one's self to the rest of the world'.[39] Judge Richard Posner argues that privacy's role is in keeping secret 'information about themselves that others might use to [the individual's] disadvantage'.[40] These conceptions frame privacy as a self-serving value. Building on sociologist Erving Goffman's idea that people commonly employ differing techniques to influence the ways they are seen by others,[41] psychologist Sidney Jourard defines privacy as 'a desire to control others' perceptions and beliefs vis-à-vis the self-concealing person'.[42] Privacy is a negative value in that it invites deceit and manipulation which diverge with broader social values. It is 'an antisocial construct ... [that] conflicts with other important values within the society, such as society's interests in facilitating free expression, preventing and punishing crime, and conducting

[39] Richard Epstein, 'The Legal Regulation of Genetic Discrimination: Old Responses to New Technology' (1994) 74 Boston U L R 1, 12.
[40] Richard Posner, *The Economics of Justice* (Harvard University Press 1981) 271.
[41] Erving Goffman, *The Presentation of Self in Everyday Life* (Doubleday 1959).
[42] Sidney Jourard, 'Some Psychological Aspects of Privacy' (1966) 31 Law & Contemp Prob 307.

government operations efficiently'.[43] For these theorists, privacy is an individual right; it possesses no value for society and indeed is a negative value that is harmful to the community. However, this conception can be refuted by examining the social benefits derived from privacy.

Traditional social approaches to privacy argue that it goes beyond the interest of the individual and enables valued social ends. Indeed, framing privacy purely in an individualistic sense often means that it becomes undervalued and is too easily subverted for social issues. This does not account for the interplay between privacy and other values, between the individual and society. After all, as John Dewey notes, 'we cannot think of ourselves save as to some extent social beings. Hence, we cannot separate the idea of ourselves and our own good from our idea of others and of their good'.[44] It is necessary to recognise the valued social ends that privacy upholds. For instance, privacy promotes professional or political relationships in much the same way that it ensures intimate ones. Social norms dictate what might be personal or intimate aspects and similarly determine which may require privacy. Privacy in this regard is contextual and only obtains its true meaning within a society.[45] In a democratic society, individual freedoms cannot be the sole concern. There must be an interest in protecting the privacy of relationships. The value of these relationships, argues Beate Roessler, is that 'these forms of social interactions and social practices have tasks and purposes that not only are morally valuable for the individuals involved, but which also directly serve to promote social integration'.[46]

---

[43] Fred Cate, *Privacy in the Information Age* (Brookings Institution Press 1997) 20.
[44] John Dewey, 'Ethics' (1908) in Boydston (ed) *The Middle Works of John Dewey 1899-1924* (Southern Illinois University Press 1978) 648.
[45] Serge Gutwirth, *Privacy in the Information Age* (Raf Casert 2002) 34.
[46] Roessler n(13) 776.

Technology has supplanted many traditional social institutions. Most shopping can be done online, many people now telecommute rather than going in to the office every day, and communications take place more often by email than by phone. However, the change in social structures does not mean that the value of privacy to society has decreased nor that the social benefits are lessened. Rather, privacy plays a subtle conservative role in reinforcing the existing social fabric. Julie Cohen examined the role of information and the increasing 'knowability' of the individual to determine what benefit privacy may offer in a world where increasing amounts of information may be known about every citizen.

> We do not need, or even want, to know each other that well. Less information makes routine interactions easier; we are free to choose, consensually and without embarrassment, the interactions that we wish to treat as less routine. Informational privacy, in short, is a constitutive element of a civil society in the broadest sense of the term.[47]

While we might choose to share more with others and while more data which is demonstrative of our inner selves might be generated via new technologies, there remains a social benefit in maintaining privacy over the information.

III. Critique of traditional privacy conceptions as a consequence of technological developments

Historically, there has been interplay between conceptions of privacy and technology with the two evolving alongside each other. In the late 19th and early 20th centuries, the development of cameras allowed for instantaneous photographs and newspapers which

[47] Cohen n(17).

'invaded the sacred precincts of private and domestic life; and numerous mechanical devices threatened to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops"'.[48] In the 1960s, this could be seen in the development of wire-tapping technologies which enabled law enforcement to listen in on conversations,[49] and the development of computers with the ability to create centralised databases of personal information.[50] The 1990s brought with it the creation of the internet and even more personal data. Paul Schwartz's article 'Privacy and Democracy in Cyberspace' looked to the links between the development of technology and the interpretation of privacy, 'From the age of computer mainframes in the 1960s to the current reign of the internet's decentralised networks, academics and the law have gravitated towards the idea of privacy as a personal right to control the use of one's data'.[51] The individual remained the controller. This followed traditional privacy interpretations rooted in liberal theories of individual rights. 'Both the focus on the individual right and the emphasis on individual control dominated much of the liberal legal and philosophical thinking about privacy during the late 1960s and through the 1980s'.[52]

However, changes in technologies which have changed concepts of information, actors, and borders are not necessarily reflective of traditional liberal theories of individual rights. Rather, they indicate a need to assess privacy's value not only in reference to the

[48] Warren & Brandeis n(6); Solove n(1) 15.
[49] Samuel Dash Richard Schwartz & Robert Knowlton, *The Eavesdroppers* (De Capo Press 1971) 25-26; Orin Kerr, 'The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution' (2004) 102 Michigan L R 801, 841.
[50] Roger Clarke, 'Information Technology and Dataveillance' (1988) 31(5) Comm of the ACM 498; Mark Poster, *The Mode of Information: Poststructuralism and Social Context* (Chicago University Press 1990).
[51] Paul Schwartz, 'Privacy and Democracy in Cyberspace' (1999) 52 Vand L R 1609.
[52] Priscilla Regan 'Privacy and the Common Good revisited' in Roessler and Mokrosinska *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015) 53.

individual, but also to the community, and determine how the norms surrounding privacy have been altered as a result of the technology. Developments in technology are indicative of a shift toward a 'networked public' wherein individual control becomes more contingent on the community. As Priscilla Regan observes, 'in a networked public, it is hard for any one person to have a level of privacy without all other persons in that network having a similar level of privacy'.[53] Privacy is shared collectively. The control and use of technology by interconnected individuals results in communities which structure how concepts such as privacy can be determined.[54] In order to effectively conceptualise privacy in the context of ICT it is necessary to acknowledge not just the role of the individual, but the role of the wider social elements which dictate privacy's value. Several issues which result from ICT and how it is handled in law have a determinate effect on privacy.

First, the relationship between law and technology often suffers from a temporal mismatch. Laws fail to keep pace with technological developments. John Perry Barlow, internet and society scholar,[55] discusses the issues with law and technology.

> Law adapts by continuous increments and at a pace second only to geology in its stateliness. Technology advances in ... lunging jerks, like the punctuation of biological evolution grotesquely accelerated. Real world conditions will continue to change at a blinding pace, and the law will get further behind, more profoundly confused. This mismatch is permanent.[56]

---

[53] *Ibid* 65.
[54] Tarleton Gillespie, 'The Relevance of Algorithms' in Gillespie Boczkowski and Foot (eds) *Media Technologies: Essays on Communication, Materiality, and Society* (MIT Press 2014) 167, 188.
[55] Andy Greenberg, 'It's been 20 years since this man declared cyberspace independence' *Wired* (2 Aug 2016) <https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/> accessed 15 Sept 2016.
[56] Roger Brownsword Karen Yeung, 'Regulating Technologies: Tools, Targets, and Thematics' in Brownsword & Yeung (eds) *Regulating Technologies* (Hart Publishing 2008).

In reconciling law with technology, the difficulty may lie in a lack of correspondence between the form of the legislation and the form the technology now takes. At other times, the original legislative purposes may no longer provide clear statutory backing for the uses to which the technology is now put. Many of the discussions about how to regulate technology focus on either 'future-proofing' the technology by making it neutral,[57] or by legislating for specific technologies which would require the law to be amended as new technologies develop.[58] The temporal discord highlighted in the relationship between law and technology is easily extrapolated to the position of privacy. Our ideas of privacy are still rooted in those traditional conceptions; but our behaviour and society has changed. The internet and permeation of technology mean that we no longer view privacy in the same way; and laws which attempt to regulate for traditional notions of privacy are ineffective.

Second, technology has fundamentally altered traditional spatial boundaries. On an individual level, this can be seen in the breaking of barriers between the public and private due to the extensive and intrusive nature of technology. 'In the past, walls, darkness, distance, time and skin were boundaries that protected personal information and helped define the self. Information about the self-resided with the individual and those who knew him or her'.[59] Information now flows freely between spheres. Things you post on Facebook to share with your friends may be reported back to your employer; thoughts and opinions posted in comments sections may be subject to scrutiny by hundreds of others. Traditional spatial distinctions cannot be maintained amongst recent technical developments. Technologies which deconstruct boundaries make it difficult for

[57] Roger Brownsword, 'So What Does the World Need Now? Reflections on Regulating Technologies' 27 in Brownsword & Yeung (eds), *Regulating Technologies* (Hart Publishing 2008).
[58] *Ibid*
[59] Gary Marx, 'Some Conceptual Issues in the Study of Borders and Surveillance' 23 in Zuriek & Salter (eds) *What Goes There? Global Policing and Surveillance* (Willan 2005) 272.

individuals to determine the context in which they are acting thereby making managing privacy more difficult.[60] As Miller notes, 'Such decontextualisation erases the distinction between what ought and ought not to be communicated'.[61] A concept of privacy which cannot account for the deconstruction of spatial boundaries cannot therefore offer sufficient protection in light of technological developments.

Similarly, the removal of the individual from the physical spaces they inhabit through their translation into discrete packets of data diminishes protections of privacy that exist in clearly delineated private spheres. By interacting and utilising various technologies, the individual becomes a collection of disparate pieces of information, known as a 'dividual'; an abstraction of oneself. In this manner, the separation of the individual and the relevant data permits interferences with privacy as the personal information is removed from the social responsibilities owed to the individual.[62] In so doing, as Vincent Miller notes, the technology can effectively circumvent the idea that data collection and processing 'can be an invasion of privacy because such data is not directly tied to an individual, which possesses rights, but to a "dividual", which does not'.[63]

An interrelated aspect to the idea of spatial bounds is the alteration in traditional borders of governance.[64] Crimes are no longer confined to one jurisdiction; perpetrators do not have to be in the jurisdiction of the crime they commit. Technologies facilitate both the commission of crimes and their detection. Didier Bigo offers a perspective on the relationship between technologies and borders in policing and the expanding use of these

[60] Alice Marwick & danah boyd, 'Networked privacy: How teenagers negotiate context in social media' (2014) 16(7) New Media & Society 1051, 1094.
[61] Vincent Miller, *The Crisis of Presence in Contemporary Culture* (Sage 2016) Loc 1249.
[62] Miller n(61) Loc 1407.
[63] Miller n(61) Loc 1414.
[64] David Johnson and David Post, 'Law and Border: The Rise of Law in Cyberspace' (1996) 48 Stanford L R 1367.

technologies to increase collaboration between various agencies, noting that they permit 'the police to discipline and punish beyond borders'.[65] Privacy intrusions may likewise occur beyond borders. It may be expected that at some stage information may be collected and used by the domestic government or law enforcement agencies. However, the nature of technology means that there is no guarantee the information won't be accessed by others outside the domestic jurisdiction. Yet despite this, the substance and purpose of privacy remains similar across modern industrialised nations.[66] Such a result points to the need to conceptualise privacy, not as a territorial or space based issue, but as one that is dependent on the technology at issue.

Third, technology has exponentially increased in its scope and overall saturation levels. Nissenbaum notes that the development of the internet has enhanced not only the ability to spread information, but also the degree to which it saturates the lived experiences of so many people in so many parts of the world.[67] Traditional notions of privacy maintain that there are some areas which are inherently private; into which there can be no interference. Historically this was possible due to limitations in the capacity and resources of technical systems which prevented interferences into areas. However, technological developments have removed these barriers. As more and more conduct occurs via information technology systems, there are very few instances in which some data isn't generated, whether it is simply purchasing groceries or reading a newspaper. The use of technological devices such as cell phones further contributes to the removal of these barriers. 'Prior to the digital age, people did not typically carry a cache of sensitive

[65] Didier Bigo, 'Globalized (in)security: the Field and the Ban-opticon' in Bigo and Tsoukala (eds) *Terror, Insecurity, and Liberty: Illiberal Practices of Liberal Regimes after 9/11* (Routledge 2008).
[66] Solove n(1) 187.
[67] Nissenbaum n(16) 53.

personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception'.[68]

Contributing to the potency of these technologies, is the capability to store the information, to analyse it, and to access it for later use. The scope and saturation levels presented by technology allow for greater powers of investigation by law enforcement. Data allows for the generation of complete profiles, accountings of individual movements and behaviours, and determination of social circles. It is not that without these technologies these things would be necessarily impossible, but the extensive nature of the data makes them more accessible and comprehensive. Individuals' most intimate traits can be discovered through improved data analysis mechanisms; machines can know highly detailed and significant information. In a similar vein, if everything you do, see, purchase, and say creates data which can be stored, searched, accessed, or analysed, privacy cannot be protected through conceptions which rely on traditional methods of intrusion.

Finally, technology has resulted in a disappearance of the ephemeral. Technology has made it so any activity can now be recorded and disseminated regardless of whether it is occurring in the public or private sphere.[69] This has a direct impact on notions of both individual freedom and autonomy and social relationships. Cybersecurity analyst Bruce Schneier discusses the significance of the ephemeral, 'Having conversations that disappear as soon as they occur is a social norm that allows us to be more relaxed and comfortable, and to say things we might not say if a tape recorder were running. Over

[68] Notably, almost 75% of smartphone users report being within 5 feet of their phones most of the time and 12% admitting they even use their phones in the shower: *Riley v California* 134 S Ct 2473 (2014) no 13-132 [United States].
[69] Jonathan Zittrain, *The Future of the Internet* (Penguin Books 2008).

the longer term, forgetting – and misremembering – is how we process our history'.[70] Having an impermanence to conversations and interactions is valuable. 'With modern technologies, elements of the past can be preserved and offered up for visual and auditory consumption'.[71] Privacy cannot be maintained wherein every thought and action is recorded and subject to later scrutiny and judgment. To do so would be to effectively normalise the behaviour of both the individual and society.

If the current approach to privacy is not tenable in light of the technology, the necessary question is how to conceptualise a framework that both accounts for these developments, and protects against privacy violations. In assessing privacy in the ICT system, it is therefore necessary to consider the social. To consider the social elements is to broaden the interest in privacy beyond traditional thinking and expand its importance in light of the complexities of modern organisational and technological change.[72] Such an approach 'is appropriate, intellectually defensible, and vital', argues Regan, 'given the trajectory of current surveillance activities, whether taken in the name of national security, public safety, or consumer choice'.[73]

Assessing the interplay between ICT systems and privacy requires an understanding of the changes upon people and societies brought about by the technological transformation and the harms, benefits, and impacts on social and cultural values. The changes in information types, actors, and transmission principles, are areas wherein Nissenbaum orients her approach to contextual integrity. The thesis uses Nissenbaum's approach as the starting point for analysis of the impact of these technological changes on the value of

[70] Schneier n(29) Loc 1978.
[71] Marx n(59) 272.
[72] Thomson n(2); Scanlon n(8); and Rachels n(27) each grapple with this issue
[73] Regan n(52) 55.

privacy, in order to assess whether the changes are justifiable, and to determine, where a violation of privacy is established, effective prescriptive measures to ensure that privacy is adequately protected under future legislative developments.

IV. Defining Contextual Integrity

Each of the previous conceptions of privacy fails to ensure privacy in light of communication technologies. It is necessary to establish a conception which can account for these developments in order to determine how to address any privacy violations which result from technological developments. Any such framework must be able to balance these developments with the wider social interests in the prevention and detection of crime. Part of the failing of the previous conceptions results from trying to apply a singular framework which can relate to all the various circumstances in which privacy is engaged. Daniel Solove argues against viewing privacy in such a manner, maintaining instead that privacy is better understood pluralistically.[74] Such an approach is derived from Ludwig Wittgenstein's conception of family resemblances,[75] wherein each problem has issues in common with other problems, but these issues are not necessarily the same across fields. To put it another way, privacy can be understood as representing a variety of different norms and values, and to define it, it should be examined in the context of the particular situation.

Central to the definition will be not only explaining the value of privacy, but utilising conceptual and normative resources to determine instances wherein privacy can legitimately override the end goals and purposes of the ICT system used in the investigatory powers instruments. The technical system at issue in the thesis will be

[74] Solove n(1) 40.
[75] Wittgenstein, L *Philosophical Investigations* (Blackwell Publishers 2001) ss 66.

explored fully in the following chapter. In the case of ICT systems used by law enforcement agencies, the question therefore is: what value does privacy maintain in systems of comprehensive information collection and processing? And how can it be protected when the core purpose of privacy is directly opposed to the policy goals?

Legal scholar Helen Nissenbaum created a framework known as contextual integrity to reconcile technological developments and conceptions of privacy. Nissenbaum argues for examining systems in context in order to assess the status of privacy within those systems. She defines the focus of her approach as follows:

> Finely calibrated systems of social norms, or rules, govern the flow of personal information in distinct social contexts (e.g. education, health care, and politics). These norms, which [Nissenbaum] calls context relative informational norms, define and sustain essential activities and key relationship interests, protect people and groups against harm, and balance the distribution of power. Responsive to historical, cultural, and even geographic contingencies, informational norms evolve over time in distinct patterns from society to society.[76]

For Nissenbaum, norms that are specifically concerned with the flow of personal information – transmission, communications, transfer, distribution, and dissemination – are informational or context-relative informational norms. When these informational norms are respected, then the context is preserved and when they are breached, contextual integrity is violated.[77] In essence, a contextual integrity approach looks to the informational norms to determine when a privacy violation occurs. This is done by

[76] Nissenbaum n(16) 3.
[77] Nissenbaum n(16) 140.

examining three characteristics of the informational norm: the relevant actors and the roles they play, the nature of the information, and the transmission of the information between parties.

Under Nissenbaum's framework, actors are senders of information, recipients of information or information subjects.[78] The roles these actors fulfil will be a determinate factor in ascertaining whether there is a privacy violation. In addition, the nature of the information itself will play a key role in determining any perceived privacy violation. In certain contexts, the disclosure of certain attributes can be deemed inappropriate.[79] For example, certain types of information may be innocuous at small scale but trigger privacy violations in the aggregate. Finally, the transmission principles involved may impact on informational norms ascribed to a practice. Established constraints on the flow of information may trigger privacy concerns when information is disseminated in a way that does not comport with expectations. This could be the case, for example, where information willingly shared for the purposes of receiving a service is later shared with a third party for an unrelated function.

By examining these three areas, it is possible to tell if an informational norm has been altered. 'If a new practice generates changes in these areas, the practice is flagged as a *prima facie* violation of contextual integrity'.[80] This is not to say that all technological systems which alter these categories result in a violation of privacy that must then be rectified. 'Whether the alterations amount to transgressions, and whether these transgressions are morally and politically legitimate depends, of course, on the contexts

[78] Nissenbaum n(16) 141.
[79] Nissenbaum n(16) 143.
[80] Nissenbaum n(16) 149.

in which they transpire and how they bear on relevant values, ends, and purposes'.[81] At times, the developments concerning information will better reflect current norms and values. It is only when they do not that they should then be addressed.

In determining whether the informational norms are violated in a manner that mandates further actions to protect privacy, Nissenbaum argues information types, transmission principles, and actors must be examined in light of the context in which the privacy violation is being alleged. Contexts are structured social settings with accepted characteristics; the framework of contextual integrity however does not require a singular context for its decision heuristic.[82] It is necessary to examine the multiplicity of factors which create the context. These can be derived from different arrangements of people and artefacts, the manners in which they coexist, and how they relate to one another and possess identity and meaning.[83] The wider social factors which dictate the context are significant to achieving privacy. Marwick and boyd find that context must be dynamic and responsive depending on the actors and norms at play: 'contexts are not bounded and information norms are not fixed. Instead, situations are co-constructed by all participants'.[84]

Where a new technological practice results in changes in these actors, information types, and transmission principles, the informational norms shift. The changes in these norms must be evaluated against the interests and impacts on the values and contextual aims.[85] The existence of a change does not in itself indicate the need for reform. Entrenched norms are not necessarily preferred and new informational norms can have value. As

[81] Nissenbaum n(16) 195.
[82] Nissenbaum n(16) 141.
[83] Nisenbaum n(16) 131-132.
[84] Marwick and boyd n(60) 1064.
[85] Helen Nissenbaum, '"Respect for Context": Fulfilling the Promise of the White House Report' in Rotenberg, Horowitz, and Scott (eds) *Privacy in the Modern Age* (The New Press 2015) 141.

John Stuart Mill long ago recognised: 'The despotism of custom is everywhere the standing hindrance to human advancement, being in unceasing antagonism to that disposition to aim at something better than customary'.[86] Any assessment of the changes in informational norms must be balanced against other issues and rights. For the purposes of the thesis, these norms will be assessed against the aims of law enforcement in collecting and processing the information. The shift in norms will be weighed against the benefits in using the communications data.

In looking at what must be done it is important to acknowledge that privacy is dynamic and changing. It is through this evaluation that the framework of contextual integrity can offer a mechanism for developing prescriptive recommendations for the system. 'Contextual integrity offers a diagnostic tool with *prima facie* explanatory and predictive capacities, providing a more highly calibrated view of factors relevant to privacy than traditional dichotomies such as public/private'.[87] By providing this level of analysis, the values and aims that need to be provided for in future legislation governing the use of ICT systems can be identified and enshrined.

V. Privacy in Context: Information Communications Technologies and Law Enforcement

To establish the conception of privacy which will be utilised in this thesis, it is first necessary to determine the informational norms that apply to the context of ICT. Subsequent chapters will then determine whether the policies of law enforcement and intelligence agencies are violating these norms by utilising the technology for data

[86] Mill n(12) 87.
[87] Nissenbaum, 'Respect for Context' n(85) 157.

retention, access, and analysis. A violation will result in a privacy intrusion which must be mitigated in subsequent legislation.

a. Context

For the purposes of this thesis, the informational norms will be assessed in the context of the ICT system which will be the focus of the following Chapter. Contexts are defined as structured social settings which account for both individual and social characteristics. In socio-technical systems, contexts are the shared 'properties of respective media, systems, or platforms whose distinctive material characteristics shape – modify, magnify, enable – the character of the activities, transactions, and interactions they mediate'.[88] Systems are composed of legislation, organisations, and artefacts. Systems contain characteristics which define their activities, and these characteristics are defined by the social structures and roles in which they are situated. In the context of the ICT system, norms are defined by the characteristics that shape both communication and information processing. Traditional communications systems (i.e. landline phones, postal mail, etc.) imposed distinctive properties on communications. Systems that utilise mobile and internet technologies have modified many of these traditional characteristics, as will be evidenced in the analysis of these systems in Chapters 3 to 5. 'If properties of technical systems and platforms define contexts, then a principle that supports *respect* for contexts presumably implies that policies should be heedful of these defining properties of systems and platforms'.[89] The thesis argues that the investigatory powers regime governing the

[88] Nissenbaum, H 'Respect for Context as a benchmark for privacy online: what it is and isn't' 272 in Roessler and Mokrosinska *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015) 282.
[89] *Ibid*

current ICT system is not responsive to the structured social settings in which it is oriented; regulations apply frameworks from outdated contexts to new technologies.

b. Roles/actors

Tied in to the concept of context are roles and actors. Nissenbaum defines roles as 'typical or paradigmatic capacities in which people act in contexts'.[90] Linked to this concept is the idea of comportment, or the kind of behaviour shown in various roles relative to what is expected.[91] Informational norms look to the roles of various actors to determine when a breach has occurred. A breach can occur if there has been a shift in principal actors, or if the purpose of the actors has changed. Nissenbaum structures informational norms with regard to actors which 'affirms intuitions that the capacities in which actors function are crucial to the moral legitimacy of certain flows of information'.[92] An actor who operates outside the accepted role calls into question the legitimacy of the action. Solove stresses the need to focus on the relationships in which information is transferred and the use to which it is put, as changes in that relationship necessarily impact on issues of intimacy, confidentiality, and power dynamics.[93]

In terms of ICT, there has been a shift in actors and the traditional relationships found in this context. The Government is no longer the principal actor in the imposition and application of mechanisms which interfere with communications data, whether by active surveillance or passive monitoring. This role is being played by CSPs. 'Ostensibly non-criminal justice institutions are being called upon to augment the surveillance capacities

[90] Nissenbaum, *Privacy in Context* n(16) 133.
[91] Gary Marx, 'Coming to terms: the kaleidoscope of privacy and surveillance' in Roessler and Mokrosinska (eds) Social *Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015) 32.
[92] Nissenbaum n(16) 142.
[93] Solove n(1) 48.

of the criminal justice surveillance system'.[94] The technologies at issue here are normally developed and administered by private entities. Political scientist Henry Farrell observed, 'much of our life is conducted online, which is another way of saying that much of our life is conducted under rules set by large private businesses'[95] which are not subject to the traditional limitations that would inhibit government action.

This change in the role of the actors facilitating privacy intruding measures is demonstrative of different norms than are traditionally associated with surveillance and monitoring when done by law enforcement. For example, individuals often consent to these actions when they are done by private companies, typically to obtain some form of benefit or service offered. 'Usually when we mind that information is shared, we mind not simply that it is being shared but that it is shared in the wrong ways and with inappropriate others'.[96] The ability of individuals to opt in to technologies which result in increased information collection and processing is significant. People who choose to disclose information in order to derive a certain benefit can consent to that information being known.[97]

Where individuals consent to share information with private actors and the information is then accessed and used by government without their consent, the roles of the actors and expectations have changed. The distinction between the end users of data is significant in that the purpose of the data and the impact of its use (whether through general collection, aggregation, or analysis) is different depending on who processes the data.

---

[94] Kevin Haggerty & Richard Ericson, 'The surveillant assemblage' (2000) 51(4) Brit J of Sociology 606.
[95] Schneier n(29) loc 944.
[96] Nissenbaum n(16) 142.
[97] Although it may be arguable whether this consent argument can still stand with the ubiquitous nature of computing. In essence, requirements which have come to inhabit our everyday life, from providing information to apply for jobs, get free Wi-Fi, use basic websites, means that there is no longer an option in many instances. Whether this negates the ability of individuals to consent is an interesting subject and one that deserves more time than I am able to devote to it here.

Indeed, law enforcement and intelligence agencies will have very different goals for the data, will process it for different reasons, and will use it to elicit different information. Law enforcement is expected to behave in a certain manner in the context of communications surveillance and monitoring; for instance, they are expected to follow certain steps, such as obtaining judicial authorisation. However, where private actors are co-opted into these roles, these safeguards do not necessarily apply. This has a direct impact on the informational norms we associate with information and communications technologies.

c. Information Types

Changes relating to the information type or attribute are also a determinate factor on informational norms. The nature of the information dictates its accepted norms. In that regard, consideration must be given to who the information concerns and with whom it is shared; what the information is about; and its scale and scope. In the context of the ICT system, the nature of the communications data collected and processed will strongly influence informational norms and the evaluation of those norms against privacy interests. Writing in 1988 Roger A Clarke found that, 'one of the most practical of our present safeguards of privacy is the fragmented nature of present information. It is scattered in little bits and pieces across the geography and years of our life. Retrieval is impractical and often impossible'.[98] This distinction no longer holds. Changes in the attributes of information occasioned by developments in technology have made it more accessible and comprehensive. The nature of communications data fundamentally shifts the traditional limitations of data that existed when it was decentralised and discrete

[98]Clarke n(50) 498.

packets of information. As a result, the changes in information types must be evaluated when ascertaining whether the entrenched norms are still relevant to the ICT system.

d. Transmission Principles

Under the framework of contextual integrity, the third factor which is assessed in determining informational norms is classed as the transmission principles. Transmission principles concern the constraint on the flow of information. Relevant to this is how the information is distributed and the scope of its dissemination. This is frequently dictated by the structure of the technologies. Lawrence Lessig's book *Code: Version 2.0* draws on this idea, arguing that it is the architecture of technology which dictates its norms.[99] For Lessig, the norms created in cyberspace are different than those in 'real' space; the latter conform to traditional societal ideals whereas the former may not. The difference in norms in cyberspace versus real space can be demonstrated in early interpretations of how cyberspace was meant to function. Early iterations of cyberspace called for pseudo anonymization to promote free expression and speech, and this was enabled through the code which established the technology. Unlike in real space, privacy was similarly incorporated, with many applications allowing for individuals to use services without placing any identification or authentication requirements.[100] However, these norms are not necessarily replicated in current communications technologies.

e. Norms

In evaluating the preceding characteristics, the significant factor will be how they have impacted on norms. Norms in this context are defined as principles which prescribe and proscribe acceptable action and practices. They may define the relationships among

[99] Lawrence Lessig, *Code and Other Laws of Cyberspace: Version 2.0* (Basic Books 2006) 432.
[100] *Ibid*

roles, e.g. between the government and the individual, and thereby the power structures that characterise social context.[101] The traditional governing structure of cyberspace and the internet has changed. So too have traditional mobile telephony applications. The original versions of cyberspace, which saw it as a place free from regulation and governance have not endured. Rather, a governing structure exists, albeit one that is enforced by private entities, allowing these private actors to dictate the normative principles of technologies. The significance of the extensive scope, lack of defined spatial constraints, and relative dominance of the technology means that these normative constraints can have both online and off-line effects. In that instance, it is important to look to what norms are being reinforced by technology.

In providing for norms which relate to information collection and processing, the impact of these practices must be acknowledged. Julie Cohen acknowledged the effect the constant monitoring that occurs as a result of persistent data collection can have on individuals. '[P]ervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream' by constraining the acceptable spectrum of behaviour and resulting in a 'subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines'.[102] Similarly, Spiro Simitis highlights the role in personal information in enforcing standards of behaviour.[103] Thus the development of these technologies has allowed for the expansion of systems which allow for persistent monitoring which impacts on behaviour and social values, including, and especially, privacy. Yet legislative policies which traditionally subject

[101] Nissenbaum n(16) 133.
[102] Cohen n(17) 1426.
[103]Spiro Simitis, 'Reviewing Privacy in an Information Society' (1987) 135 U Pa L R 707.

these processes to limitations in scope and protections from abuse have not similarly developed.

f. Values

In order to determine whether the entrenched norms are indeed acceptable for the context, it is necessary to then determine what values the system is seeking to promote. These values are also known as the goals, purposes, or ends around which a context is oriented. Traditionally, information processing regimes possessed clear values; the information was collected and processed for a particular service. Law enforcement access to these systems had, at its core, the detection of suspects and the eventual prosecution of crime as their aims. However, increased data flows, coupled with social and historical developments have altered the traditional objectives of the ICT policies enacted by law enforcement.

There has been 'a shift in thinking in which crime is no longer viewed as an aberration but rather a normal condition of late modern society and therefore all citizens come under suspicion'.[104] This has resulted in shifts in the values of technology from tools of detection to tools of prevention. 'Contemporary surveillance is characterised by its lack of particularity in that it is an intelligence-gathering tool used before the relevant enforcement agency has any suspicion that a particular individual has been involved in crime'.[105] Scholars such as Zedner, Ericson, and Haggerty note that the shift from a post-crime to a pre-crime society has fundamentally changed the nature and aim of policing

[104] Ben Bowling Amber Marks & Cian Murphy, 'Crime Control Technologies: Towards an Analytical Framework and Research Agenda' in Brownsword & Yeung, *Regulating Technologies* (Hart Publishing 2008) 53.
[105] Daniel Solove, *Nothing to Hide: the False Trade-off between Privacy and Security* (Yale University Press 2011) 61.

and emphasises security.[106] Van Brakel observes that the change is not merely temporal but also has implications for relevant actors as well: 'In a pre-crime society the responsibility for security against risk is not just the responsibility of the State but extends to a larger group of individual, communal, and private actors'.[107] Proponents argue the extended scope and scale of the information processing activities which affect privacy interests are required in this atmosphere of 'global insecurity'.[108] Interests such as privacy must be balanced against the community values which want security, and more often than not the former are forfeit to this security interest. This raises the question, of what safeguards can be put in place to address the issues raised by these technologies and adequately ensure that the values ascribed are preserved, particularly in the wake of increasingly invasive technologies.

VI. Conclusion

The preceding analysis has found that privacy, in light of technological developments, is best conceptualised in a contextual manner. Such a conceptualisation requires an analysis of the components of informational norms that are engaged in a contextual analysis of ICT systems which indicate areas where technologies utilised by law enforcement and intelligence agencies can alter entrenched norms. The question then becomes whether changes in these norms represent a violation of privacy that must be regulated for in future or whether they can be justified by relation to values they enshrine. In order to determine which of these two scenarios prevails, it is necessary to examine the specific nature of the technologies and their capabilities. The following

[106] Lucia Zedner, 'Pre-crime and post criminology?' (2007) 11(2) Theoretical Criminology 261, 262; Richard Ericson & Kevin Haggerty, *Policing the Risk Society* (Clarendon Press 1997) 41.
[107] Rosamunde Van Brakel and Paul De Hert, 'Policing, surveillance and law in a pre-crime society: Understanding the consequence of technology based strategies' (2011) 20 J of Police Studies 163, 166.
[108]Richard Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (Oxford University Press 2006) 171, 141.

analysis will proceed by setting the context by defining the ICT system and norms and values within it and then examine the technical systems utilised by law enforcement and intelligence agencies, focusing on the procedures of retention, access, and analysis. In each of these areas, the impact on informational norms will be established by investigating how the preceding criteria have been affected.

CHAPTER 2: THE INFORMATION COMMUNICATIONS TECHNOLOGY SYSTEM

I. Introduction

To assess privacy using contextual integrity, it is necessary to establish the context in which it is being evaluated and the norms which exist within that context. To that end, this chapter evaluates privacy in the context of the ICT system. Law and technology are complex and interrelated structures which are elements of a system which reflects a co-constructed relationship. Technologies cannot be divorced from society but that does not mean they are purely social constructs.[1] An interpretation of technology which accounts for the role of the social is necessary but insufficient; further elements must be considered, including the technology itself and the organisational and legislative actors which direct its use. Each of these elements plays a crucial role in dictating the capabilities and limits of technology. It is argued that the interpretation of the relationship between law and technology is best informed by the systems theory approach of Hughes which is employed in the following analysis. As will be shown, this theory provides for a way to assess how technology shapes and is shaped by society.

This chapter will define what is meant by a technological system through reference to the literature, before examining the ICT system at issue in the thesis. The theory employed here allows for the assessment of the impact of technology on individual and social levels, which will help determine the informational norms associated with the concept of privacy identified in the Chapter 1. This will also underpin the development of prescriptive measures to apply to the system which address how to incorporate the new

[1] Torin Monahan, 'Questioning Surveillance and Security' in Johnson and Wetmore (eds), *Technology and Society: Building our Sociotechnical Future* (MIT Press 2008) 545.

role of CSPs in the criminal justice process and how to tackle the fundamental changes to the nature and use of information in the system.

This chapter sets out the rationale behind adopting Hughes's systems theory approach in four parts. Part I begins by assessing the relevant literature on law and STS approaches to technologies. These theories are critiqued with regard to its benefits and shortcomings in understanding ICT. This analysis will establish that the systems theory approach of Thomas P Hughes is the strongest method with which to critique the ICT concerning communications data found within the investigatory powers instruments. Following that, Part II will then apply Hughes's systems theory to information communications technology, examining the technological evolution of the system, as well as problems in the system that were overcome both technologically and socially. Part III will identify the basic legislative, organisational, and technical elements which form the system. Finally, in Part IV, the social structures affected by the co-construction of the system are assessed by examining these structures and the impact of the system on their development. The foundational work of this chapter establishes the role of the system and the various factors which must be taken in to account in assessing its efficacy. This chapter dictates the context, in the form of the structured social settings, in which the conception of privacy established in Chapter 1 must be assessed. As such, this chapter and Chapter 1 form the theoretical basis on which the analysis of the data retention, access, and analysis set forth in Chapters 3 to 5 will be based.

II. Law and STS Approaches to Technology

In order to determine the most appropriate theory for analysing the ICT system in the investigatory powers regime it is necessary to examine the interplay between law and technology. Falling under the broad heading of Science and Technology Studies (STS),

these approaches offer a way in which to examine the interdependency between law and technology and consider how these two areas are co-produced. Such approaches account for the reciprocal relationship between the two distinct fields. As Faulkner et al recognise, 'Technology can be seen to be both an object of the law, and as a means (sometimes unintended) of engendering new laws and legislative understandings'.[2] The aim of this section is to highlight the different perspectives and approaches that are taken in the wider field of STS when assessing this relationship in order to establish the approach most useful for interrogating that relationship in the context of the ICT system. In determining this relationship, the context of the developments will be significant, as the mechanisms for interpreting these interactions will be contingent on the context in which they occur. Here, in the context of ICT used for law enforcement, the respective norms and values embodied by the system differ from the use of ICT for purely private purposes. STS approaches lend themselves to the normative considerations raised by the development of ICT and the implications of those developments on privacy by enabling the analysis of the wider social and political factors which underpin the legal changes.

The use of STS approaches for assessing the relationship between law and technology have enabled the examination of the nature of legal processes and the production of technologies.[3] Social factors are incorporated into these developments through their potential and eventual uses and implementations.[4] An STS approach recognises that these developments and their impacts cannot be understood in a purely linear and static

[2] Alex Faulkner Bettina Lange & Christopher Lawless, 'Introduction: Material Worlds: Intersections of Law, Science, Technology and Society' (2012) 39(1) J of L and Soc 1, 16.
[3] Emilie Cloatre Martyn Pickersgill, 'Introduction' in Cloatre and Pickersgill (eds) *Knowledge, Technology and Law* (Routledge 2014) 4.
[4] Mark Flear Martyn Pickersgill, 'Regulatory or regulating publics? The European Union's Regulation of Emerging Health Technologies and Citizen Participation' (2013) 21 Medical L Rev 39, 48.

manner. Law and technologies in this area are co-produced.[5] As Sheila Jasanoff notes, knowledge in this area 'embeds and is embedded in social practices, identities, norms, conventions, discourses, instruments and institutions – in short, all the building blocks of what we term of the social'.[6]

Scholars working within STS frameworks, particularly those in the field of criminal justice, have analysed heretofore unchallenged areas, including those which posit the self-corrective ability of science and technologies; the rule of law in these areas; notions of expertise; and the infallibility of evidentiary claims related to evidence derived through technological means.[7] However, it is necessary to explore how the criminal law concepts overlap with the development of information communications technologies. Such an interpretation allows for an assessment of how these technologies shape and mediate interactions between individuals and wider society. As Yeung notes, 'information communications technologies, like other artefacts, shape and mediate our relationship with the world around us and, over time, we come to perceive the world through the lenses that our artefacts create'.[8] Changes in these perceptions impact on not only the technologies themselves, but also the way individuals react with social units. This assessment can be broadened out to wider concepts of power and the rule of law by

[5] Sheila Jasanoff, 'The idiom of co-production' in Jasanoff (ed) *States of Knowledge: The co-production of science and social order* (Routledge 2004).
[6] Jasanoff n(5) 3.
[7] Barbara Prainsack, 'Unchaining research: processes of dis/empowerment and the social study of criminal law and investigation' in Cloatre and Pickersgill (eds) *Knowledge, Technology and Law* (Routledge 2014) 72. In particular, there is extensive literature which assesses this relationship in the field of DNA. See: Franklin Zimring, *The Contradictions of American Capital Punishment* (Oxford Uni Press 2003) 170; Jay Aronson Simon Cole, 'Science and the Death Penalty: DNA, Innocence, and the Debate over Capital Punishment in the United States' (2009) 34(3) Law and Social Inq 603; Sheila Jasanoff, 'Just Evidence: The Limits of Science in the Legal Process' (2006) 34 J L Med & Ethics 328; Tal Golan, *Laws of Men and Laws of Nature* (Harvard Uni Press 2004).
[8] Karen Yeung, 'Hypernudge: Big Data as a mode of regulation by Design' (2017) 20(1) Info, Comm, & Soc 118, 129; Peter-Paul Verbeek, 'Moralising Morality: Design Ethics and Technological Mediation' (2006) 31(3) Science, Technology & Human Values 361; Julie Cohen, *Configuring the Networked Self* (Yale Uni Press 2012).

allowing for an examination of the salient factors which underpin developments in these areas.[9] As such, an STS approach, by emphasising the construction, use, and implementation of technologies, allows for an evaluation of how these factors can be better accommodated in the legal process.

Within STS there is a wide body of scholarship which demonstrates the need to study the impact of these developments on social practices and how they embed or establish various structures and authorities.[10] Such accounts look to certain technologies or practices and assess how various factors in their development and use reflect back upon the social. For example, in the work of sociologists Trevor J Pinch and Wiebe Bijker, the development of the bicycle is analysed. This analysis works 'on the assumption that the social lies *behind* and directs the growth and stabilisation of artefacts'.[11] Artefacts do not have to be singular inventions; they can be component elements of a wider technology, and encompass both the physical and nonphysical. In this theory, particular technologies remain background factors against which human, social, and political conflicts take shape. For Wiebe and Bijker, technologies exist to solve dilemmas as they are defined by relevant social groups; a problem only exists when there is a social group for which it constitutes a 'problem'.[12] These social groups consist of organised and unorganised groups of individuals, institutions, and organisations. What is important for the existence of a social group is that the group gives the same meaning to the technological

[9] Shiela Jasanoff, 'Ordering knowledge, ordering society' in Jasanoff (ed) *States of Knowledge: The co-production of science and social order* (Routledge 2004) 16; Flear n(4) 48.
[10] Shiela Jasanoff, *Science at the Bar: Law, Science and Technology in America* (Harvard Uni Press 1995); Andrew Pickering, *The Mangle of Practice: Time, Agency, and Science* (Uni of Chicago Press 1995).
[11] John Law, 'Technology and Heterogeneous Engineering: The Case of Portuguese Expansion' in Bijker Hughes & Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012) 107.
[12] Bijker and Pinch develop the theory of the social construction of facts and artefacts through an analysis of the development of the bicycle. (Wiebe Bijker & Trevor Pinch, 'The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other' in Bijker Hughes & Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012) 17.

'artefact'.[13] Once the group is identified, the question becomes what problems they have with the artefact and the proposed solutions the group may have. Both the problems and solutions may present conflicting technical requirements, conflicting solutions to the same problems, or other moral conflicts amongst the social group as different social constructions and cultural interpretations are considered.

In determining the role of the social Pinch and Bijker argue that their 'account – in which the different interpretations by social groups of the content of artefacts lead by means of different chains of problems and solutions to further developments – involves the content of the artefact itself'.[14] This means that in developing the artefact, each social group may focus on the problem most relevant to their own interests; the focus will not be the same across social groups and the actions taken will vary accordingly.[15] These methods of problem solving are referred to as technological frames.[16] This idea of problem solving is broadly interpreted as recognising the problem, defining strategies for solving it, and setting out the criteria for solutions that must be met for it to be accepted by the relevant social group.[17] 'The concept of a technological frame is intended to apply to the *interaction* of various actors. Thus it is not an individual's characteristics, nor the characteristics of systems or institutions; frames are located between actors, not in actors or above actors'.[18] These technological frames therefore structure the attribution of the shared meaning the social group gives to the artefact. As more members of a social

[13] These artefacts are broadly defined.
[14] Bijker and Pinch n(12) 36.
[15] In Bijker and Pinch's analysis (n(12)) of the development of the bicycle for example, two groups identified were those who wished the cycles to go faster, and women and elderly men. The former favoured developments in the evolution of the cycle which increased speed. The latter were more concerned with those developments that improved safety.
[16] Wiebe Bijker, 'The Social Construction of Bakelite: Toward a Theory of Invention' in Bijker Hughes & Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012) 164.
[17] *Ibid* 164.
[18] *Ibid* 168.

group or additional social groups interact with the artefact, this gives rise to and structures the methods of the groups, giving rise to a technological frame. In this method, it is not possible to divorce those actors from the technology; as Gillespie notes these 'groups of actors...also have a stake in that technology's operation, meaning, and social value'.[19]

In structuring the meaning that a social group gives to an artefact, there is necessarily a reflection of social principles. Actors will play different roles depending to which social group they belong. Boundaries are blurred as actors and artefacts are socially situated in different ways depending on the social group under consideration. For example, a user will give different meanings to an artefact than an inventor or engineer. However, that user can simultaneously be a creator and an engineer; the analysis will differ depending on whether the technology is examined in the context of a consumer or a developer. The resultant shared meaning that a group gives to the artefact is a consequence of distinct factors. Langdon Winner incorporates this understanding in his discussion of a social approach to technological development, noting that the development of technology will advance certain social interests over others.[20] 'In the process by which structuring decisions are made, different people are situated differently and possess unequal degrees of power as well as unequal levels of awareness'.[21] This can serve to reinforce the current social structure and this reinforcement can be indicated in the decisions of societies to favour certain technologies over others. These choices may not reflect the most efficient nor equitable use of the technology.

[19] Tarleton Gillespie, 'The Relevance of Algorithms' in Gillespie Boczkowski and Foot (eds) *Media Technologies: Essays on Communication, Materiality, and Society* (MIT Press 2014) 167, 182.
[20]Langdon Winner, *The Whale and the Reactor* (U of Chicago Press Books 1986) 26.
[21]Winner n(20) 28.

However, these approaches which assess the meaning of the social in these contexts does not mean that the social is placed above other factors. STS approaches to the study of these technological artefacts have consistently refused to place causal primacy upon the social.[22] The assessment of the social in the approaches of Pinch and Bijker among others does not imply that 'social reality is ontologically prior to natural reality, nor that social factors alone determine the workings of nature'.[23] As the study of the role of the social in the development of technologies has matured, approaches here have required a reimagining of what is a complex subject. STS links with the study of technology to determine how the two must be linked together, acknowledging the importance of people, individuals, and preferences.

At the other end of the spectrum of the analysis between technology and society lies the technological determinist approach. Technological determinism views technological change as an independent factor which then causes social change.[24] As Marx and Smith state in the context of technological determinism, 'a complex event is made to seem the inescapable yet strikingly plausible result of a technological innovation'.[25] Technology is seen as an outside force upon society which directs social growth, rather than the other way around. Seeing these technological artefacts as conditioning the social allows for an analysis of how the devices transform everyday life.[26] The impact of the technological on the social can either be 'soft' or 'hard', with the former holding that the technology

[22] Jasanoff n(9) 19; See also: Karen Knorr-Cetina, *Epistemic Cultures: How the Sciences Make Knowledge* (Harvard Uni Press 1999); Pickering n(10); Steve Woolgar, *Knowledge and Reflexivity: New Frontiers in the Sociology of Knowledge* (Sage 1988).
[23] Jasanoff n(9) 19.
[24] Jay Kesan and Rajiv Shah, 'Deconstructing Code' (2003-2004) 6 Yale L J 277, 283.
[25] Leo Marx and Merritt Roe Smith (eds), *Does Technology Drive History?: The Dilemma of Technological Determinism* (MIT Press 1994) ix.
[26] Winner n(20) 6.

drives social change but is still responsive to social pressures, and the latter arguing that the technology develops completely independently of any social constraint.[27]

Whether 'hard' or 'soft', technological determinism argues that technology develops in a fixed, naturally determined sequence. In order for there to be technological evolution, development must follow a sequential and determinate course.[28] Under the technological determinist approach, technology displays a structured history and does not develop in any great leaps. Each era has a limited capacity of, and constraint on, the accumulated stock of available knowledge. Technology develops through the gradual expansion of that knowledge.[29] This expansion is similarly related to the existence of other technologies, as there is an interrelatedness between technologies without which certain innovations would not work. Heilbroner discusses this, stating that 'the competence required to create such a technology does not reside alone in the ability or inability to make a particular machine ... but in the ability of many industries to change their products or processes to "fit" a change in one key product or process'.[30]

It is in this developmental relationship that the interplay between society and technology becomes apparent. However, in contrast to those approaches which would argue that it was the technological frame of a relevant social group which required the development of the technology, the determinist approach argues that it is through the technology that certain social or political characteristics are imposed on the society itself. Heilbroner argues that this imposition of a pattern of social relations on society can be demonstrated

[27] Merritt Roe Smith, 'Technological Determinism in American Culture' in Marx and Roe Smith (eds) *Does Technology Drive History?: The Dilemma of Technological Determinism* (MIT Press 1994) 2.
[28]Robert Heilbroner, 'Do Machines Make History' in Johnson & Wetmore (eds), *Technology and Society: Building our Sociotechnical Future* (MIT Press 2008).
[29] Heilbroner n(28).
[30] Heilbroner n(28).

by examining the functional processes of technology.[31] Keith Kelly similarly notes that 'each rise in social organisation throughout history was driven by an insertion of a new technology'.[32]

Technological determinism is frequently used to analyse historical examples to demonstrate how technologies fundamentally altered the social. While not necessarily determinist themselves, historical accounts can illustrate this concept. Lynne White assesses the development of the stirrup and how it fundamentally changed warfare and subsequently history by enabling the creation of an efficient cavalry.[33] Karl Marx links the development of the steam mill to industrial capitalism.[34] Francis Bacon listed three "practical arts" that changed the world: the printing press, gunpowder, and the magnetic compass. Bacon went on to argue that 'no empire, no sect, no start seems to have exerted greater powers and influence in human affairs than these mechanical discoveries'.[35] The impact of technology on the social is readily apparent in these examples. The determinist approach arguably offers a needed corrective to constructivist interpretations which tend to ignore the role of technology in effecting social change.[36] It accounts for the significant impact of technologies on society and the ability of technologies to determine social and cultural changes.

However, despite its value for assessing the impact of technology on the social, it is too circumscribed in its remit to prescribe an accurate analysis of the development of

[31] Heilbroner n (28) argues that this can be done through an examination of the labour force and the hierarchical organisation of work, for example in the development of a factory system over a traditional artisan workforce.
[32]Kevin Kelly, *What Technology Wants* (Penguin Books 2010) 39.
[33]Lynne White, *Medieval Technology and Social Change* (Oxford University Press 1966) 135.
[34]Karl Marx and Friedrich Engels, *Collected Works* (Vol 5 Lawrence & Wishart 2010) 516.
[35] Francis Bacon, *The Instauratio magna Part 2: Novum organum and Associated Texts,* (Rees & Wakely (eds), Clarendon Press 2004) 168.
[36]Thomas P Hughes, 'Technological Momentum' in Johnson & Wetmore (eds), *Technology and Society: Building our Sociotechnical Future* (MIT Press 2008) 141.

technology and its relationship with social norms. As has been noted by scholars such as Prainsack, STS approaches have worked to counter this narrative that technologies are only limited by those humans using them.[37] Technologies necessarily incorporate the social into their development; they do not operate in a vacuum. Technology, and in particular information technology, cannot be divorced from the social, economic, and political context in which it exists.[38] Engineers, corporations, regulatory agencies, politicians, lawyers, and users all contribute to technological development. These social entities mediate the technology and enable its introduction and assimilation into society.[39] If the focus is only on the technology, then the material conditions and social environments through which they are produced and operate are obscured. It is therefore necessary to adopt an approach which accounts for the role of both the technological and the social.

In order to avoid the limitations of deterministic approaches, it is necessary to adopt an approach which accounts for the co-production of law and technology.[40] According to Faulkner, 'Whether we study the material (scientific and technological) basis of law or its translation into practice, we find that the malleabilities of the social and the of the material to be interdependent'.[41] In order to effectively trace the interdependency of these elements, this thesis posits that the systems theory approach developed by Thomas P Hughes offers the best theoretical underpinning for understanding the development of the ICT system and its subsequent impact on legal and policy developments. The reasoning for selecting this approach will now be discussed.

---

[37] Prainsack n(7) 74.
[38] David Lyon, 'A Sociology of Information' in Calhoun Rojek and Turner (eds) *The SAGE Handbook of Sociology* (SAGE 2005) 224.
[39] Daniel Sarewitz, 'Pas de Trois: Science, Technology, and the Marketplace' in Johnson and Wetmore (eds), *Technology and Society: Building our Sociotechnical Future* (MIT Press 2008) 276.
[40] Jasanoff n(9) 20.
[41] Faulkner et al n(2) 16.

a. Thomas P Hughes's approach to Systems Theory

It is necessary to adopt a theoretical approach which can comprehend the complexity of an evolving technological system.[42] This is due to the interrelated nature of technology and society; technology may at times be the cause of social change or conversely the result. Consequently, technology is both shaped by and shapes society. Any analysis of technology which fails to account for this will be limited in its practical applicability. To address this, a third method of analysis is needed: systems theory. The approach to systems theory used in this thesis finds its roots in the work of Thomas P. Hughes. For Hughes the social and technical interact within the technological system.

In order to adequately assess the growth of technological systems, Hughes argues for a systems approach which accepts that technology and society cannot be divorced from one another. Instead, as Priscilla Regan notes, these systems are 'complex interdependent systems of technical artefacts, cultural factors, social actors, and situated meanings'.[43] Artefacts in the system acquire their meaning from the spheres and ideologies in which they operate; the relation of one artefact to another provides a meaning in that particular context.[44] However, meanings may change between artefacts as their relation to one another differs depending on a variety of factors, such as the time and place where the interactions occur. As Manuel Castells summarises, 'Appropriate technologies must be available at the time and place in which their need is directly felt by people and their organisations. Thus there is synergistic interaction between technological discovery and social evolution'.[45] The development of the system cannot

[42] Hughes n(36).
[43]Priscilla Regan, 'Privacy and the Common Good: Revisited' in Roessler and Mokrosinska (eds) *Social Dimensions of Privacy* (Cambridge U Press 2015) 51.
[44]Helen Nissenbaum, *Privacy in Context* (Stanford University Press 2010) 167.
[45] Manuel Castells, *Communication Power* (Oxford University Press 2013) xxvi.

occur in a vacuum and it is not possible for there to be a unitary interpretation of elements relevant to a given context.[46] Further, there is a levelling of the system; neither the social nor the technology can be placed above the other. All aspects of the system can be interconnected and their various elements can be examined without necessarily assigning greater value to one over the others.

In establishing the system, all artefacts which function and interact with other elements are relevant. Those artefacts are socially constructed because they are invented and developed by system builders and their associates.[47] Hughes broadly classifies the various subsections of artefacts as physical, organisational, and legislative. Each of these categories plays a role in the process of creating technology, preferring certain ends and incorporating different designs into the technology to reinforce or reconfigure particular values. These artefacts can be either physical or nonphysical, and relate to the construction of the system by interacting with other artefacts, all of which contribute in some way to the common system goal.[48] 'Technological systems solve problems or fulfil goals using whatever means are available and appropriate; the problems have to do mostly with reordering the physical world in ways considered useful or desirable, at least by those designing or employing a technological system'.[49] The limits of the technological system are those which result from control exercised by artefactual and human operators.[50]

[46]Andrew Balmer, 'Telling Tales: some episodes from the multiple lives of the polygraph machine' in Cloatre and Pickersgill (eds) *Knowledge, Technology and Law* (Routledge 2014) 106.
[47]Thomas P Hughes, 'The Evolution of Large Technological Systems' in Bijker Hughes & Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012) 46.
[48]Hughes n(47) 45.
[49] Hughes n(47) 48.
[50] Hughes n(47) 48.

The construction of artefacts lends itself to the argument that social considerations are incorporated into the development of the technological system.[51] Technologies are designed with certain users and uses in mind and will promote the values of those users; if a different group gains control over the technology, they can redefine its use and alter the values. This can be clearly demonstrated by the ICT system which was designed to enable communications between users but has been co-opted as a law enforcement mechanism, favouring public over individual interests. Law notes 'that those who build artefacts do not concern themselves with artefacts alone but must consider the way in which the artefacts relate to social, economic, political, and scientific factors'.[52] All of those various factors and considerations are in themselves interrelated and potentially malleable as the system grows, incorporates goals, and solves different problems.

However, despite the ability of systems theory to address the argument that technology is co-constructed with society, it is not without its critics. Principal to these criticisms is the idea that the system presupposes a distinction between the system itself and its environment. In systems theory, the world outside of technological systems that shapes them, or is shaped by them, is the environment. The environment is not part of the system because it is not under the control of the system. Actor Network Theory (ANT) aims to address these issues within systems theory. In ANT, the actor network is composed of heterogeneous elements that are linked but not necessarily in a stable and well defined fashion, allowing the networks to redefine and transform their elements. Scholars such as Michel Callon and John Law advocate for this approach, noting its

[51] Hughes defines the social as the world that is not technical (physical artefacts and software); made up of institutions, values, interest groups, social classes, political and economic forces.
[52] Law n(11) 106; MacKenzie similarly notes that 'artefacts bear within their design the imprint of the full range of circumstances (including economics and politics) within which the system builders worked'. Donald MacKenzie, 'Missile Accuracy: A Case Study in the Social Processes of Technological Change' in Bijker Hughes and Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012).

ability to apply not just to interactions at a given time but to any subsequent developments as well.[53] ANT also removes the reliance on the social focus of the elements driving technological change. Law states that, 'Other factors – natural, economic, or technical – may be more obdurate than the social and may resist the best efforts of the system builder to reshape them. Other factors may, therefore, explain better the shape of artefacts in question and, indeed, the social structure that results'.[54] ANT therefore argues that social elements should not be distinguished from those that are natural or technological in the analysis. What is important is not necessarily the role one element plays above others, but the patterns and conflicts that are revealed between different types of elements, some social and some otherwise.

Actor network theory is distinct but not wholly different from the core of systems theory. Rather, it differs in the way it approaches conflict between elements. Whilst the environment is treated as outside the system, MacKenzie argues that Hughes' approach 'sensitises us to the fluidity of the boundary between technological systems and their environments, particularly the way in which it raises the question of the extent to which systems builders seek to mould their environments to facilitate the growth of their system'.[55] The role of the actors in producing the system is significant as they dictate the constraints of organisational, political, and economic matters. The technology is a product of this context, and a contributing factor to the development of these matters.[56]

As a result, for the purposes of this thesis, the systems theory approach to dealing with the development of technological systems is better suited to an analysis of the ICT found

[53] Michel Callon, 'Society in the Making: The Study of Technology as a Tool for Sociological Analysis' in Bijker Hughes, and Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012) 94.
[54] Law n(11) 110.
[55] MacKenzie n(52) 208.
[56] Zednek Smutny, 'Social informatics as a concept: Widening the discourse' (2016) 5 Journal of Information Science 42, 681.

in the investigatory powers instruments, particularly in light of the focus on their impact on privacy. An account of the impact on privacy which looks purely at the social implications of the technology would fail to take into account the significant changes in the data collected as a result of technological developments. These include developments which have increased the scale and scope of data, diminished traditional boundaries, and removed temporal limitations. Utilising a technological determinist approach would similarly be insufficient. Such an approach relies too much on the role of the technology at the expense of the social factors which have contributed to its development. Therefore, in order to effectively assess the impact on privacy the analysis must be twofold. First, the social must be considered as the conceptualisation of privacy in this thesis is rooted in social norms and values. Second, the changes wrought by the development of the technology and their impact must be assessed. As Kaplan finds,

> By weaving together the technical and the social, we get a more complete picture of human societies and technologies as well as the ways we are both independent of and dependent upon our machines. Creating new interpretations of these relationships helps reveal the relativity and necessity behind our technological choice and thus opens up prospects for better, more informed decisions about our current and future technologies.[57]

Hughes's approach to systems theory, which takes into account both these factors without preferring one over the other, is therefore the chosen method for the analysis of the information communications technology herein.

[57] David Kaplan, *Readings in the Philosophy of Technology* (Rowman & Little 2004) xv.

III. Applying Hughes's approach to information communications technology

While the preceding analysis examined the overarching principles which guide systems theory, this section will address the specific issues that need to be considered when applying the framework to the analysis of an ICT system. Key to this framework is the development of the system itself. Whilst the technological determinist approach argues for the linear progression of technological development, a systems theory approach recognises that systems do not necessarily evolve in this manner. There are various phases which overlap and backtrack as the system develops, including invention, development, innovation, transfer, growth, competition, and consolidation.[58] Systems are driven by various inventions, which can be classed as radical, requiring the establishment of a new system; or conservative, such as changes and developments to an existing system that are necessary to enable the system to improve and expand.[59]

As the system develops, the incorporation of the social becomes more readily apparent, as economic, political, and social characteristics are embodied in the system to enable it to function in the world.[60] As systems begin to embody these relevant characteristics, they become more entrenched and adaptations become more incremental. It is therefore difficult to have a dramatic overhaul or complete abolition of a system along the lines of what may occur through 'radical inventions'; it is more likely that invention in the system will be conservative. Jeremy Bentham described this tendency to conform to entrenched systems in the legislative context: 'when new laws are made in opposition to a principle established by old ones, the stronger that principle is, and the more odious will the inconsistency appear. A contradiction of sentiment results from it, and disappointed

[58] Hughes n(47).
[59] Hughes n(47) 56.
[60] Hughes n(47) 56.

expectations accuse the legislator of tyranny'.[61] This respect for custom and principle can lead to a sense of security.

Yet as technology continues to develop, the question remains of how to address those components, entrenched as they may be, when they fall behind or out of phase with other elements in the system. Social customs and principles are insufficient to allow these elements to remain in the system, and systems must be able to account for different environments and developments or risk losing all value.

Hughes classifies components that are out of sync with the system as reverse salients. Development of the system is achieved through identifying these reverse salients and attempting to correct them. Much like in the social constructivist theory, different groups may identify different reverse salients as they prioritise goals and identify elements as barriers to progress. However, it cannot be said that even members within the same group will agree on the barriers to achieving their goals or the best means to accomplish them.[62] In the case of the ICT system used for investigatory powers purposes, the reverse salients will differ depending on whether the artefact, communications data, is examined from the legislative perspective which incorporates law enforcement's views, or from the organisational viewpoint which examines the problems from the perspective of communications service providers.

Similarly, the reverse salients do not have to be physical artefacts in themselves; they may be part of the organisational or legislative elements. For example, when there is a need to pass new investigatory powers legislation, the legislative process could be interpreted as a reverse salient which needs to be addressed. In doing so, the different

[61] Jeremy Bentham, *Theory of Legislation* (Vol 1, Weeks Jordan & Co 1840) 182.
[62] MacKenzie n(52) 206.

interpretations of political parties, NGOs, and technology companies must be considered before passing law which requires changes to the technologies. Conversely, the reverse salients could be technological advances that render elements of the current legislation ineffective or obsolete. The key aspect is that there is an element of a system which has fallen out of phase with the others. The existence of reverse salients in the technological system at issue herein is readily apparent. The growth of large ICT systems has altered information gathering, analysis, and distribution, as well as the types of information, actors, and any conditions or constraints on information flows.[63] Such changes directly impact upon traditional conceptions of privacy. The components which currently exist at the legislative and organisational level are ill suited to deal with these developments. Solutions to these reverse salients are necessary to ensure the continuing effectiveness of the system.

As the systems overcome their reverse salients, allowing them to grow and develop, they acquire what Hughes calls 'technological momentum'. The systems 'have a mass of technical and organisational components; they possess direction or goals; and they display a rate of growth suggesting velocity'.[64] Constant similarly recognises this idea of technological momentum, arguing that it is the culture of technology that enables this momentum; the development of technology along previously defined trajectories contributes to this concept.[65] People, whether they are in the form of individuals, governments, corporations, etc., can direct the development of new technologies, but as these systems gain momentum, they move beyond the control of these entities. It

[63] Helen Nissenbaum, 'Respect for Context as a benchmark for privacy online: what it is and isn't' in Roessler and Mokrosinska (eds) *Social Dimensions of Privacy* (Cambridge University Press 2015) 294.
[64] Hughes n(47) 70.
[65] Edward Constant, 'The Social Locus of Technological Practice: Community, System, or Organisation?' in Bijker Hughes and Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012) 223.

requires a powerful external force to alter technologies once they possess this momentum.[66]

Altering technologies becomes increasingly more difficult once the system has embodied various political, economic, social, and value components. As Koops states: 'Because technology is often irreversible – once it is developed and applied in society, it is hard to fundamentally remove it from society in those applications – the process of developing technology is a key focus when normativity is at stake'.[67] Once the artefacts or elements of a system become entrenched, they embody the characteristics and norms present at their inception, rather than changing their characteristics.[68] Other barriers to change, once the system has gained technological momentum, exist as well. Technology is highly path dependant and it becomes expensive to undo or alter entrenched characteristics.[69] Legislative delays contribute to the technological momentum and the longer the system is left to develop unchecked, the more difficult it becomes to change the path of the technology.[70]

It is argued that the ICT system has acquired substantial momentum along these lines. The system encompasses a variety of modes of communications, technical components, legislative aims, and organisational structures, all of which embody the various political, economic, social, and value components. The communications data at issue in this thesis, and the norms and characteristics ascribed to it still relate to the socially constructed character of data that existed prior to technological developments which

[66] *Ibid*.
[67] Bert Jaap Koops, 'Criteria for Normative Technology: The Acceptability of 'Code as Law' in light of Democratic and Constitutional Values' in Brownsword and Yeung (eds) *Regulating Technologies* (Hart 2008) 166.
[68] Hughes n(47) 70.
[69] Alan Rozenshtein, 'Surveillance Intermediaries' (2017) 70 Stanford L R 1, 133.
[70] Patricia Bellia, 'Designing Surveillance Law' (2011) 43 Ariz St L J 293, 320.

fundamentally altered information norms. In the following Chapters, these norms will be determined with regard to the specific retention, access, and analysis processes to which they relate. An analysis of ICT utilising systems theory is necessary to determine how to correct for technological momentum in amending the current regime governing communications data in order to ensure that privacy, as conceptualised in Chapter 1, can be protected when information is collected and processed by law enforcement.

IV. The elements of the information communications technology system

The following provides a brief synopsis of the elements of the ICT system. Broadly speaking, the technological system is that which enables communications between entities, who are themselves both components and constructors of the system. The relationship between the constituent parts of the system are at times technical, at times social, and at times both. The interconnections between the relevant elements may not be readily apparent but it is hoped that through the elaboration of the elements of the system, it will be possible to demonstrate the links, reverse salients, and potential future developments. The following defines the technological system through reference to the legislative mechanisms, organisational elements, and artefacts retained, accessed, and analysed in the system itself.

a. Legislative Mechanisms

Legislative artefacts such as Acts of Parliament and statutory instruments are an integral part of the technological system. These components are creations of social groups, including politicians and law enforcement, and can embody the motivations and principles of the entities for whom those legislative proposals are drafted. Principally, the ICT system examined relates to the investigatory powers instruments utilised to collect, retain, provide access to, and analyse communications data by law enforcement

agencies in discharging their duties. The legislative developments in this area are motivated both by the increasing capabilities of technology and by the demands of law enforcement to create new and adapt existing technologies to further criminal justice aims. The use of technology is ubiquitous in contemporary criminal justice, both in its use by law enforcement and in motivating the development of further technologies.[71] It would therefore be impossible to adequately address the development of the system without reference to legislative elements and the groups responsible for creating them.

One particular area wherein the relationship between technology and law enforcement has been altered as a result of legislation is in the regulation of information across traditional jurisdictional bounds. Technological developments have enabled the free flow of information across the globe and frustrated law enforcement attempts to access relevant data as it is no longer necessarily held in in the domestic jurisdiction. Further, distinctions between national and international, military and police, intelligence gathering, and police investigations have been blurred and/or merged. As Marx notes, 'with increased internationalisation and globalisation of crime, terror, and social control, the meaning of national borders and foreign and domestic actions is less clear'.[72] The lack of traditional jurisdictional distinctions results in legislation which increases requirements on states to place restrictions on ICT providers working in their jurisdictions to ensure domestic rules are embodied within the architecture of the technology.[73] One such rule prevalent in the use of ICT by law enforcement under the investigatory powers instruments is to impose positive obligations on the intermediaries

[71]Ben Bowling Amber Marks & Cian Murphy, 'Crime Control Technologies: Towards an Analytical Framework and Research Agenda' in Brownsword and Yeung (eds) *Regulating Technologies* (Hart 2008) 60.
[72] Gary Marx, 'Some Conceptual Issues in the Study of Borders and Surveillance' in Zureik and Salter (eds) *What Goes There? Global Surveillance and Policing* (Willan 2005) 25.
[73]Joel Reidenberg, 'States and Internet Enforcement' (2003-2004) 1 U Ottawa L & T J 213, 218.

who facilitate communications to retain and process this information, rather than having law enforcement undertake these processes themselves. These intermediaries are able to capture information that passes through their systems, even if that information originates or has an end destination outside of the jurisdiction. This allows law enforcement to minimise the resources they themselves have to dedicate to collecting and analysing this material and assists them in dealing with potential offenders who are dispersed across traditional boundaries.[74]

In order to facilitate these processes and provide legal backing for their implementation and use, legislation works to dictate the development of technology. Specific examples of the legislative development are examined in the following chapters. However, for now it is sufficient to note that one of the primary motivating factors behind these legislative developments is that the information is available consistently and efficiently to those relevant law enforcement agencies.[75]

Practical examples from other jurisdictions demonstrate the legislative application of regulations to technologies utilised for law enforcement purposes and can be a useful comparator for the UK system. In the United States, a shift in the infrastructure of telephone networks meant that wiretapping would become more difficult. As a result, in 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA) to cope with the transition of telephone technology from analogue to digital networks. When the networks changed, law enforcement lost the ability to tap phones.[76] The Government responded by passing legislation which required private companies to facilitate law enforcement's ability to conduct electronic surveillance.[77] Lawrence Lessig

[74] *Ibid* 224.
[75]Explanatory Memorandum to the Data Retention (EC Directive) Regulations 2009, 3.
[76]Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) Harvard L R 531.
[77] Communications Assistance for Law Enforcement Act 1994 [CALEA] (US) 47 USC.

notes that in this case, 'The industry created one network architecture. That architecture didn't adequately serve the interests of government. The response of the government was to regulate the design of the network so it better served the government's ends'.[78] This requirement did not require a wholesale change in the structure of the IT system, rather, companies were placed under a legislative obligation to comply with requests.[79]

If the data must be modified or retained in specific circumstances based on the laws of the country, then that directly impacts on the technological processes which concern that data. This pattern can be transposed to the situation in the UK where the technologies through which communications services are provided are required to incorporate elements which serve the interests of State security and law enforcement. Such requirements can similarly be witnessed when the legislature amends or authorises practices in the wake of judicial rulings.[80] The impact of the legislative components of the system on the development of the technology and the embedding or alteration of social norms is demonstrated through the analysis in Chapters 3 to 5. In order to facilitate this analysis, it is necessary to examine legislative restrictions placed on CSPs at the organisational level; on the artefacts of the data retention systems, access systems, and analysis provisions; and at the legislative level on the public authorities accessing and analysing the data.

[78]Lawrence Lessig, *Code 2.0* (2 edn, Createspace 2009) Loc 1228.
[79] CALEA n(64) ss 1001-1002; More recent developments in this area relate to data localisation laws which mandate the retention of data within the territorial jurisdiction of a State. See: Anna Sashina, 'Russian Data Localisation Law: commentary of the Ministry of Communications' (*Bird & Bird*, 28 Aug 2015) < https://www.twobirds.com/en/news/articles/2015/global/russian-data-localistation-law> accessed 11 Nov 2016; Paulo Trevisani, 'Brazil Lawmakers Remove Controversial Provision in Internet Bill' *Wall Street Journal* (Brasilia, 19 March 2014) < https://www.wsj.com/articles/SB10001424052702304026304579449730185773914> accessed 11 Nov 2016.; and Manuel Maisog, 'Making the Case against Data Localization in China' (IAPP 20 April 2015) < https://iapp.org/news/a/making-the-case-against-data-localization-in-china/> accessed 11 Nov 2016; and Decree on Management, Provision, and Use of Internet Services and Online Information (No 72/2013) (Viet).
[80] Bellia n(70) 305.

b. Organisational Elements

Technological systems similarly possess an organisational element which must be incorporated into any analysis of the system. Constant succinctly sets out the key roles of the organisation in the system, 'Purchase or use of almost any modern technology is mediated by the complex organisations that are required to integrate the knowledge and resources necessary to produce and distribute that artefact or service'.[81] Organisations are system creators, incorporating prescribed elements into the system. These elements may reflect legislative aims; technical limitations of the artefacts; and incorporate distinct social, economic, and political values. As such, organisational factors fundamentally shape the system. It is similarly important to note that organisations are themselves shaped. An organisation may have a hierarchy which reinforces a particular social structure, possesses functionally differentiated departments which have different aims, and so on.[82] All of these organisational variables will have an impact on the development and functioning of the system. The primary organisational element discussed in the context of the ICT system and the investigatory powers instruments is that of communications service providers (CSPs). These are private commercial bodies which are required to fulfil law enforcement and national security aims concerning retention, access, and analysis, as established by the legislative mechanisms.

CSPs embody several forms with the primary objective of enabling communications between at least two parties. To that end, entities such as phone companies and internet providers are all communications providers. In Britain these companies are private entities and have been since the establishment of telephone services in this jurisdiction

[81] Constant n(65) 225.
[82] Constant n(65) 226.

thereby providing them with long established networks and significant structural power.[83] The ICT system at issue in this thesis is focused on the communications provided by phone and internet companies, with particular emphasis on mobile telephony and internet communications. Mobile telephony and the internet have become the dominant modes of communication and therefore their role in the system is dramatically increasing. The use of traditional post and land line telephones has significantly decreased.[84]

It is necessary to establish what fall under the definition of communications service providers of internet and mobile communications to determine the significance of these organisational structures for the system. In terms of mobile communications, traditional mobile phone service providers are CSPs for the purposes of this analysis. In the UK, there are four dominant providers which account for 85% of mobile communications.[85] These providers facilitate communications by providing both phone and text services, as well as providing data packages which allow individuals to communicate using the internet. As of 2016, 71% of adults in the UK owned a smartphone which enabled these communications.[86] In fact, smartphones have overtaken laptops and home computers as the dominant computing device. Similarly, providers of internet broadband fall under the category of CSPs. In the UK, 86% of homes have internet access.[87] Much like mobile phone service providers, there are four broadband providers which dominate the UK

[83] Monica Horton, *The Closing of the Net* (Polity Press 2016) 72.
[84] The OFCOM report of 2016 demonstrates the change in modes of communication. Addressed letter volumes fell by 3.7% in 2016. The majority of adults in the UK (56%) prefer emails rather than letters wherever possible. Nearly half of all adults (47%) say that they only use post if there is no alternative. OFCOM, *Communications Market Report 2016* (4 Aug 2016) < https://www.ofcom.org.uk/__data/assets/pdf_file/0024/26826/cmr_uk_2016.pdf> accessed 12 Jan 2017, 219.
[85] OFCOM n(84): These are respectively EE with a 29% market share, O2 at 27%, Three at 11%, Vodafone at 19%, and other at 15%.
[86] OFCOM n(84) 179.
[87] OFCOM n(84) 179.

market, accounting for 87% of all broadband services provided in the UK.[88] As a result, it is difficult to communicate via mobile telephony or the internet without engaging with one of these services.

The definition of CSPs does not only apply to these traditional communications entities however. Non-traditional service providers may similarly be considered CSPs. Social media platforms like Facebook, Twitter, and Snapchat provide communications services over the top (OTT) of the traditional mobile and broadband services. Indeed, these modes of communication are becoming increasingly prevalent. In 2016, UK adults spent nearly half of their time on social media communicating using these over the top communications services.[89] Messaging apps are frequently seen as substitutes in themselves for traditional telecoms services and are fast overtaking email and text as the primary modes of communication.[90] The shifts in types of communications and their overall saturation in society will have a significant impact on the social norms assigned to this type of information. Developments in the system which create new types of information, assign new roles to actors, or change the way the information is shared will be evidenced in the following chapters. The subsequent analysis of the role of the organisational element of the system will demonstrate areas for prescriptive changes in order to better ensure privacy where communications data is collected and processed. Any assessment of the organisational role of CSPs must look at how they dictate the development of the system and determine what their responsibilities should be to ensure adequate protections of fundamental rights.

[88] OFCOM n(84) 151. These are respectively BT with 32%, Sky at 23%, Virgin at 19%, and TalkTalk at 13%.
[89] OFCOM n(84) 185.
[90] OFCOM n(84) 182.

The position of the organisation is privileged. Organisations both facilitate communications and provide the structure through which the communications data can be caught by the established legislative mechanisms. The inability to communicate without potentially engaging at least one of these CSPs is significant. Even if it is possible to avoid communicating with one, the scope of the CSPs is so exhaustive that it is likely the communication will be caught by another. Arguably, this is the principal reason that the CSPs have been co-opted into the law enforcement processes. These entities offer a logical target for the criminal justice process; they can act as a point of control to collect and filter information and process it in a manner most useful to law enforcement aims.[91] As the market becomes increasingly dominated by a smaller number of large companies, the ability to employ legislative mechanisms to regulate it increases.[92] However, this ability can be frustrated by jurisdictional issues as the increasingly globalised nature of CSPs means that providers of the OTT services (i.e. Facebook, Twitter, WhatsApp, etc.) are based overseas making it difficult for the UK enforcement agencies to obtain the data.[93] The organisational element of the system thereby must interact with the legislative to guarantee the required access and control.

c. Technical Artefacts

Here the technical refers to artefacts in the system (both with physical and non-physical forms) that function as components and interact with the other elements to satisfy the common system goal. These artefacts 'embed key human rights and relevant decision-

[91] Niva Elkin-Koren & Eldar Haber, 'Governance by Proxy: Cyber Challenges to Civil Liberties' (2016) 82 Brooklyn L R 105, 111.
[92] Lessig n(78) Loc 1365.
[93] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (Stationary Office 2015) 4.15. This can be contrasted with the case of landline calls which are made through a UK CSP to which the owner subscribes and therefore the information can be collected and retained easily.

making capacities'.[94] For the application of investigatory powers within the ICT system, the principal artefact of analysis is classed as communications data generated by mobile telephony and internet communications. This data interacts with other artefacts such as the retention systems, analysis technologies, and access procedures. The aim here is to provide an overview of the artefacts employed in the investigatory powers instruments which are embodied in the ICT system for retaining, providing access to, and analysing communications data.

Communications data is the principal constituent artefact of the system and provides the information which then interacts with other system elements. Organisational structures and legislative mechanisms concern themselves with this data and its relation to the other components of the system. Communications data has been a constitutive element of information communications technology throughout the development of the system, enabling law enforcement agencies to discover the who, where, when and how of communications. Traditional methods such as postal communications classed this information as envelope data, i.e. the information written on the outside of an envelope which concerned who sent and received the communication and the relevant addresses of the parties. Similarly, in the context of telephone communications, police utilised techniques such as metering to obtain records of numbers dialled from a phone, without the consent of the subscriber.[95] The data generated through these traditional communication methods was facilitated by an organisational structure which required the retention of this information for private purposes. David Anderson noted this in his analysis on communications data: 'historically, there has been a high availability of the

[94] Council of Europe, 'Recommendation of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries' CM/Rec (2018) 2.
[95]Yaman Akedeniz Nick Taylor & Clive Walker, 'Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State Surveillance in the age of information and rights' (2001) Feb Crim LR 73.

communications data that investigators required. Typically the subscriber to a telephone number and the call log that went with it were the information needed; these were also the basis for the service provider to charge their customer'.[96] The needs of the organisation and law enforcement complemented one another and therefore the ICT system was able to incorporate these considerations in the treatment of communications data.

However, fundamental requirements set out in legislation, organisational changes, social changes, and technological advances to the structure mean the traditional processes employed are no longer fit for purpose. The system has been transformed by the growth in service providers, changes in traditional modes of communication, fragmentation of services, changing business models, and jurisdictional issues. This has been coupled with changes in the nature of the communications data itself as a result of the inclusion of data generated by internet and mobile phone communications. Communications data is now broadly classed into three areas: traffic data, location data, and subscriber information. Many of these categories overlap with the traditional categories of data captured, however, due to the scale and scope of the ICT system, the implications of this data are far greater.

Traffic data is that which can be used to identify the person, device, location, or address from which a communication is transmitted.[97] It is also used to identify the technical system which enabled the transmission of the communications.[98] This means that traffic data incorporates not just information on individual users, but information on the components of the system more generally. Arguably, this element was present in the

[96] Anderson n(93) 7.52.
[97] Regulation of Investigatory Powers Act 2000 s 21(4)(a).
[98] RIPA n(97) s 21(6).

traditional communications data provisions as phone companies were able to note the user of the phone, the address of the account, and what network they used to facilitate the communications. However, the data in the current ICT system goes farther than this analysis by also providing for the capture of Internet Protocol (IP) addresses. Yet IP address capture does not enable the same goals of identifying users and devices as traditional traffic data did. The technology which enables the capture of IP addresses does not necessarily provide an accurate and consistent location as companies assign the same IP address to multiple users.[99] Nor is the person who holds an internet account necessarily the one using a particular device in a particular location. This is particularly apparent in the case of publicly available Wi-Fi networks wherein many users will use the same account, making it difficult for law enforcement to utilise this information to achieve their aims. When IP addresses are able to be tied to an end user, the effect on the user is much more substantial than when that information was gathered in the rather circumscribed manner through traditional telephony and postal means. Daniel Solove highlights the issue: 'although who you call on the phone can be quite revealing, how you browse the Web exposes even more of your private life, for it reflects what you're thinking and reading'.[100] The legislation requires that the technology develop to permit the capture of this data. However, the norms of the ICT system must develop as well to incorporate these concerns rather than applying established norms to this new and potentially more revealing category of data.

Location data is another element of communications data that forms a crucial component of the ICT system. Broadly speaking, this data concerns the movement of individuals

[99] Anderson n(93) 4.18. This is known as Network Address Translation and is a technique used by CSPs to streamline their service but which allows IP addresses to be shared by multiple customers simultaneously.
[100]Daniel Solove, *Nothing to Hide: The False Trade-off Between Privacy and Security* (Yale University Press 2011) 159.

which is elicited from mobile and connected devices. The traditional mechanisms for gathering such data would have been through targeted active surveillance by law enforcement or through the use of devices such as GPS trackers attached to vehicles. These powers were limited by practical concerns; it was not possible to follow a person everywhere. Location data has altered this, creating a new source of data through the functions of mobile phones which accompany the individual the majority of the time. Location data is further enhanced by individuals' use of over the top services such as Twitter and Facebook which can reveal the user's location.[101]

Service use and subscriber information represent the third category of communications data. Service use information relates to the frequency and time a person used a service and which service they used. This information parallels that found in an itemised phone bill and doesn't depart dramatically from traditional data types in that regard. Where the difference lies is in the business models at the organisational level which no longer require this type of information. Subscriber information relates to all the other information that the customer provides, such as their address, telephone number, email address, etc. which is necessary in order for them to receive the service.

These technological developments concerning communications data possess implications for the traditional mechanisms employed and therefore call into question the effectiveness of the current system infrastructure. The development of the capabilities concerning communications data, through increased collection, retention, access, and analysis capabilities can therefore be classed as a reverse salients of the system, as the data has fallen out of sync with the original functions of the system. Data plays an increasing role in society. The systems which concern this data do not merely collect

[101] Anderson n(93) 4.30.

information but create comprehensive records whereby associations can be tracked, personal interests identified, and personality characteristics revealed.[102] The growth and development of the system is enabled by the mobility of information. To an extent, this is an inevitable consequence of the development of the system. Cybersecurity expert Bruce Schneier refers to the 'smog of data' as a natural by-product of technology, 'data is the exhaust of the information age'.[103] The creation of data is a consequence of the technologies and the needs of CSPs and Governments to be able to interact with those technologies.[104] The organisational and technological advances have created a resource for the State to utilise. A problem therefore presents when the other aspects of the system (particularly those in the legislative subsection) fail to keep pace with the changing nature of the data. This creates the need to change the system.

Communications data interacts with other artefacts in the system through a variety of mechanisms. The first of these interactions is classed as the collection and retention processes which are necessitated by legislative demands and installed and managed through the organisational entities. The objective of these systems is to provide 'a general technique for representing data and processes in a manner that can be stored, retrieved, and reproduced'.[105] Retention therefore collects and collates the data to facilitate the abilities of the police, following access procedures, to trace acts and events. Brighenti notes that the need to introduce traceability for the data reflects a variety of institutional aims and enables the possibility of retrospective investigations.[106]

[102]Bruce Schneier, *Data and Goliath* (WW Norton & Co 2015) Loc 298.
[103] *Ibid* Loc 246.
[104] Lessig n(78) argues that the architecture of the Web itself contributes to the development of the technologies.
[105]Jonah Bossewitch and Aram Sinnreich, 'The end of forgetting: strategic agency beyond the panopticon' (2012) 15(2) New Media & Society 224.
[106]Andrea Brighenti, 'Democracy and its visibilities' in Haggerty and Samatas (eds) *Surveillance and Democracy* (Routledge 2010) 62.

Retrospective investigations are a crucial element for law enforcement and one of the principal aims of these mechanisms. Under previous instruments, organisations could only retroactively retain data for limited business purposes; this data was not necessarily the data most useful for law enforcement, nor was the retention standardised across the industry.[107] This meant that collection of communications data could only begin once a crime was committed and a suspect identified. It therefore couldn't be used to provide evidence of locations at the time of the crime which could be used to confirm or disprove alibis or to establish connections between suspects at the time of or preceding the offence. The broad collection and retention has thereby enabled the end of the ephemeral. Technology enables the recording and dissemination of activities, regardless of where it occurs in physical space.[108] As Gary Marx observed, 'With modern technologies, elements of the past can be preserved and offered up for visual and auditory consumption'[109] thereby enabling the investigative powers of law enforcement.

Once the information is collected and retained, the data can interact with other components of the system through the analysis procedures applied by law enforcement to the data. The changes in the nature of the data and inclusion of collection and retention processes in the system mean that this data can be searched easily, collated, cross-referenced, and correlated with other information.[110] This increases the value of the data and its potential to facilitate legislative aims. Helen Nissenbaum remarked on the significance of this, 'information begets information: as data is structured and analysed it

[107]See: Anti-Terrorism, Crime, and Security Act 2001 and the Data Protection Act 1998.
[108]Jonathan Zittrain, 'Perfect Enforcement on Tomorrow's Internet' in Brownsword and Yeung (eds) *Regulating Technologies* (Hart 2008).
[109] Gary Marx, 'The Declining Significance of Traditional Borders (and the Appearance of New Borders) in an Age of High Technology' in Droege (ed) *Intelligent Environments* (Elsevier Science 1997) 484.
[110]Bruce Schneier, 'Security Trade-Offs Are Subjective' and 'Technology Creates Security Imbalances' in Johnson and Wetmore (eds), *Technology and Society: Building our Sociotechnical Future* (MIT Press 2008) 534.

yields implications, consequences, and predictions'.[111] Much like it enables retrospective investigations, the technology similarly promotes proactive policing through the meanings it can derive from this information. As Judith Rauhofer notes the development of proactive policing is accompanied by trends towards the use of more technical surveillance devices by law enforcement agencies.[112]

Therefore the ability to process and analyse communications data is valuable to the legislative mechanisms of the system. The question is to what extent is that aim sufficient to overrule other considerations concerning limitations on the processing and use of communications data. In his piece on 'Dataveillance' Roger Clarke identifies issues with processing data which has been collected and retained in this aggregated manner and discusses the importance of knowing the context of the data in the analysis.[113] Interpreting and analysing the data removes it from its original context wherein it is simply the by-product of using a service. It is used to construct meanings about the data, which go beyond what the data was originally meant for thereby introducing a reverse salient into the ICT system. Where individuals' data is increasingly subjected to inclusion and processing through the system, the impact on individuals' rights affected must also be accounted for; too often, these rights do not keep pace with the development of the technology.[114]

Technical artefacts are not the only component of the system that should be considered here. Individuals can also be classed as components necessary for the system to function.

---

[111] Nissenbaum n(44) 37.
[112] Judith Rauhofer, 'Privacy and Surveillance: Legal and Socioeconomic Aspects of State Intrusion into Electronic Communications' in Edwards and Waelde (eds), *Law and the Internet* (Hart Publishing 2009) 554.
[113]Roger Clarke, 'Information Technology and Dataveillance' (1988) 31(5) Comm of the ACM 498.
[114] Rosamunde Van Brakel R and Paul De Hert, 'Policing, surveillance and law in a pre-crime society: Understanding the consequence of technology based strategies' (2011) 20 J of Police Studies 163.

For example, a phone which enables communications does not only require the device and the communication; humans are needed as well. There can be no communications, and therefore no communications data, without individuals present to transmit and receive them. As Haggerty and Ericson note these individuals are more socially and spatially mobile and entangled with a wider range of institutions, and, notably for the purposes of this thesis, CSPs.[115] Such entanglements are inescapable in the modern world and the sole choice of individuals is with the technical artefacts they chose to interact with. However, individuals may also be classed as systems creators as they necessarily develop the technical elements of the system, create and develop legislative and organisational structures, and become the operators of the various entities. These individuals incorporate normative elements into the artefacts in the system.[116] It is therefore impossible to examine the creation of a technological system without discussing the norms and social structures that are incorporated into the system and informed by the normative elements of the system components. It is to these elements that the discussion now turns.

V. The impact of the information communications technology system on the social

Legislative, organisational, and technical components are sufficient to create one technological system, but these factors have implications beyond their constructed elements; consideration must be given to the role of the social in the creation of the system. The effect of this technological system can be found in the surveillance mechanisms it embodies, including the watching, monitoring, recording, and processing of information. The development of the ICT system has affected the traditional

[115] Richard Ericson & Kevin Haggerty, *Policing the Risk Society* (Clarendon Press 1997) 42.
[116]These normative elements are referred to as 'code'. See Lessig n(78) and Koops BJ n(67).

processes utilised by law enforcement for investigations and resulted in a shift in informational norms concerning privacy. It is necessary to assess these norms against the development of the system itself as notions of acceptability co-evolve over time with social, cultural, and institutional settings.[117] To begin to assess the impact, it is therefore necessary to examine the traditional norms which applied to police monitoring and analysis of personal information. It is only in this context that the role of the system itself can be detected.

Investigatory powers concerning communications data are associated with several elements of the criminal justice process. Powers to access information operate in the context of *ex post facto* criminal investigations to establish what was done when and by whom. The investigatory powers are also related to surveillance in the indiscriminate monitoring and tracking of individuals enabling elements of *ex ante* investigation. Bruce Schneier succinctly describes surveillance under the old system.

> When surveillance was manual and expensive, it could only be justified in extreme cases. The warrant process limited police surveillance, and resource constraints and the risk of discovery limited national intelligence surveillance. Specific individuals were targeted for surveillance, and maximum information was collected on them. There were also strict minimisation rules about not collecting information on other people.[118]

Traditional mechanisms for surveillance therefore were limited in their capabilities and their scope; individuals were targeted and limitations enforced.

[117] Nissenbaum n(44) 140.
[118] Schneier n(102) Loc 355.

The investigatory powers regime governing communications data has the opposite effect. The distinction is described by Ben Bowling et al who perceive that 'Contemporary surveillance is characterised by its lack of particularity in that it is an intelligence-gathering tool used before the relevant law enforcement agency has any suspicion that a particular individual has been involved in a crime'.[119] Bowling goes on to discuss the 'mission creep' of technologies which occurs when techniques used for surveillance of individual suspects are developed into more general surveillance frameworks. This 'mission creep' can be influenced by a variety of factors which are external to the technology, including crises and unexpected threats to the security of the State. Such factors lead to the blurring of traditional distinctions between crime and terrorism and whose remit investigations in those areas should fall under. Legislative actions tend to react decisively and unilaterally when such events occur, resulting in powers that do not comport to traditional limitations and oversight.[120] As Cass Sunstein argues, 'in a democracy, officials, including lawmakers, are particularly quick to respond to public alarm'.[121] This leads to the widening of surveillance powers and the approval of more invasive technologies for monitoring and tracking.

In many instances, monitoring and tracking is not the direct aim but rather an inadvertent consequence of some other goal for which the system was designed. The facilitation of communications allows for the consequences of surveillance. For example, 'Whereas monitoring in an unstructured three-dimensional physical space requires significant engineering intervention...monitoring online activities requires relatively minor

[119] Bowling n(71) 61.
[120] Jon Michaels, 'All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror' (2008) 96 Cal L R 901, 907.
[121] Cass R Sunstein, 'The Laws of Fear' (2002) Harvard LR 1119, 1127.

adaptations of existing functional features'.[122] Often, the monitoring capabilities are secondary uses of the data which was originally captured for advertising, profiling, or other business purposes. This is particularly true as private companies who have a vested interest in personal information and its processing are increasingly co-opted into the surveillance process.[123]

The extension of surveillance activities under the investigatory powers instruments is enabled by the nature of the components described in the preceding section. The computerisation of data, together with the processing systems for collection, retention, and analysis, allow for more data to be captured and applied in an efficient manner. 'This efficiency is made possible by the technology which permits searches that before would have been far too burdensome and invasive'.[124] This is coupled with a greater reliance on private parties in collecting and managing the information which thereby reduces the burden on the police. All of this comes without any additional burden being placed on the individual.

The expansion of surveillance is exacerbated by the scope of the technology which is demonstrated by the inability to communicate without the technologies. It is difficult for anyone living within ordinary society to avoid the monitoring.[125] For CSPs, the architecture and business models, scale and reach of operations, and number of users, result in a market which is dominated by a few large organisations which account for the majority of communications in the UK.[126] There is a lack of choice for the individual but to accept the collection, retention, and later processing of their data. Often, individuals

[122] Nissenbaum n(44) 29.
[123] Bert Jaap Koops & Ronald Leenes, '"Code" and the Slow Erosion of Privacy' (2005) 12(1) Mich Telecom & Tech L R 335.
[124] Lessig n(78) Loc 538.
[125] Lessig n(78) Loc 3760.
[126]Regan n(43) 65 discusses this with regard to Facebook and Google. See also OFCOM n(84).

do not understand how information is processed and used and to what extent it can be used to make decisions concerning them.[127] Sociologist Valarie Steeves notes that, 'Even when people do understand the commercial models of [web]sites and accept the terms of use, they do so because it is the only way they can access the socio-technical spaces that they increasingly rely on for social connectedness.[128] The modes of communication facilitated by the organisational components of the ICT system are of fundamental importance to society and therefore there exists little opportunity to evade the monitoring mandated by the system. As these large organisational structures continue to develop, there is the potential for them to crowd out and eliminate previous social structures which limited monitoring. This is a trend identified by Langdon Winner: 'It is not merely that useful devices and techniques of earlier periods have been rendered extinct, but also that patterns of social existence and individual experience that employed these tools have vanished as living realities'.[129]

The acceptance by the individual of technologies which increase monitoring reinforces the value of these systems, particularly as the role of the individual often serves to reinforce or even shape the meaning assigned to the system. As Tarleton Gillespie observes, 'Once technologies are offered to the public ... users make them their own, embedding them in their routines, imbuing them with additional meanings that the technology provider could not have anticipated'.[130] The role of both the individual and the organisation in incorporating the technology into society reinforces Hughes's

[127]Daniel Solove, *Understanding Privacy* (Harvard University Press 2008) 182. See also Lessig n(78) Loc 3768 who states: 'The technologies of today have none of the integrity of the technologies of *1984*. None are decent enough to let you know when your life is being recorded'.
[128]Valarie Steeves, 'Privacy, sociality, and the failure of regulation: lessons learned from young Canadians' online experiences' in Roessler and Mokrosinska (eds) *Social Dimensions of Privacy* (Cambridge U Press 2015) 244.
[129] Winner n(20) 48.
[130] Gillespie n(19) 186.

argument for technological momentum, as the system develops and expands beyond the control of any of its singular components. This momentum is reinforced by the development of social systems and practices that then come to rely on the data in the system and further motivate its development.[131]

The expansive scope of the system and its technological momentum enables social control. The focus on social control can be contrasted with traditional surveillance theories based on the writings of Jeremy Bentham and Michel Foucault which focus on disciplinary societies and the panopticon. The effect of the panopticon was, according to Foucault, 'to induce ...a state of conscious and permanent visibility that assures the automatic functioning of power'.[132] This would result in changes in behaviour which conformed to broader social objectives. However, computers have fundamentally altered the nature of surveillance, arguably moving away from the traditional panoptic conception of social discipline. '[T]he conceptualisation of surveillance has expanded from keeping watch over prisoners and other unfortunates to pervasive systems employing a wide range of technologies for manipulating social behaviour and, as a consequence, impacting social values'.[133] Giles Deleuze and Felix Guattari argue that this indicates a shift from societies of discipline to societies of control.[134] In the disciplinary societies of the panopticon, spaces were static and visibility unidirectional.[135] Individuals passed from distinct enclosures where they were observed to ensure explicit behavioural norms, set by those in power, were followed.[136] Societies of control

[131] Nissenbaum n(44) 41.
[132]Michel Foucault, *Discipline and Punish* (Alan Sheridan tr, Penguin 1991) 201.
[133]David Wright et al, 'Sorting out Smart Surveillance' (2010) 26(4) Comp L & Sec Report.
[134] Gilles Deleuze & Felix Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia* (U of Minn Press 1987) 21.
[135] Gilbert Caluya, 'The post-panoptic society? Reassessing Foucault in surveillance studies' (2010) 16(5) Social Identities 621.
[136] Deleuze n(134).

acknowledge that people exist in several coexisting states; disparate arrays of people, technologies, and organisations interact across fields and traditional structures of visibility wherein the powerful observe the masses are increasingly being altered and levelled.[137]

The shift to societies of control is a result of technological advances. As Gary Marx observed: 'Control is now better symbolised by manipulation than coercion, by computer chips than prison bars, and by removable and invisible filters than by handcuffs and straightjackets'.[138] The development of technologies introduced monitoring techniques to identify parties in areas that would previously have been unwatched.[139] Disciplinary societies would not be able to fulfil this function unless the individuals passed within the bounds of their constrained system. This control is similarly being shifted to the technical elements of the system through processes like automated filtering which assigns values to communications and flags elements for further investigation.[140] Control through the system eliminates the human element, decreases costs, and removes discretionary elements which can be challenged.[141] Technologies which promote this control are therefore increasingly incorporated into the system, and those that do not meet these aims are phased out.

Similarly, the nature of the system now enables control across traditional spatial bounds impacting on social structures. Didier Bigo argues that this removal of bounds is demonstrated by the ability of control and surveillance to occur through time and

[137] Deleuze n(134).
[138] Van Brakel n(114) 175.
[139] Lessig n(78) Loc 774.
[140] Home Office, *Operational Case for Bulk Powers* (2016) < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf> accessed 15 Dec 2016.
[141] George Ritzer, 'Control: Human and Nonhuman Robots' in Johnson and Wetmore (eds), *Technology and Society: Building our Sociotechnical Future* (MIT Press 2008) 224 discusses control through technology in the context of labour at fast food restaurants.

distance, regardless of the traditional structures between the State and society.[142] Technologies create new methods for identifying and monitoring behaviour. This is enabled by the capabilities of the systems due to their scope and social saturation to trace data subjects 'through and between once-distinct social realms'.[143] Traditional boundaries, whether they are domestic or foreign, public or private, or national or international, no longer limit these powers. 'Data can now be captured, stored, processed, and accessed readily and economically, even when the facilities and their users are physically dispersed'.[144] This leads to a levelling of the powers of surveillance, as it can be undertaken and imposed by a wide variety of organisations and impact equally on individuals.

These elements inform the argument that the traditional social structures of surveillance are converging to the point that there is a surveillant assemblage which demonstrates the various arrays of people, technologies, and organisations which have become connected.[145] The principal foundation for the surveillant assemblage can be found in the works of sociologists Kevin Haggerty and Richard Ericson: 'The assemblage operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct 'data doubles' which can be scrutinised and targeted for intervention'.[146] Much like the technological system, these assemblages are composed of multiple heterogeneous objects that come together and 'work' as a functional entity.[147] It is possible therefore to utilise the concept of the

[142]Didier Bigo D, 'Globalized (in)Security: the Field and the Ban-opticon' in Bigo and Tsoukala (eds) *Terror, Insecurity, and Liberty: Illiberal Practices of liberal regimes after 9/11* (Routledge 2008).
[143]David Lyon, 'The new surveillance: Electronic technologies and the maximum security society' (1992) 18 Crime, Law, and Social Change 159.
[144]Clarke n(113).
[145]Caluya n(135).
[146] Kevin Haggerty & Richard Ericson, 'The surveillant assemblage' (2000) 51(4) Brit J of Sociology 606.
[147] Haggerty n(146).

surveillant assemblage to demonstrate the effects of the ICT system's components on the social structures which relate to surveillance practices. The relevance of the surveillant assemblage is demonstrated by the nature of the system which provides for the multiplication of sites of surveillance, deterritorialisation, automation, and changes in visibilities.

In the panopticon, the gaze of the watcher was unidirectional. Now these sites of surveillance have increased, thereby rupturing the unidirectional nature of the gaze that existed in the panopticon.[148] This is not to say that confined realms where there is a unidirectional gaze are no longer present in societies, but rather that this model is but one element in a larger field of concrete assemblages. With the surveillant assemblage '[s]urveillance becomes methodical, systematic, and automatic, rather than discontinuous, as was the case with the disciplinary technology'[149] associated with the panopticon. This reflects the Deleuzian idea that in a society of control the individual inhabits several metastable states at the same time.[150]

Similarly, this shift away from the disciplinary mechanism of the panopticon to a surveillant assemblage, is reflected in the evolution of a surveillant system which is deterritorialised. In addition to the lack of traditional territorial boundaries, the digitialisation of surveillance has deconstructed the traditional notions of bounded space that existed within the panopticon. As William Bogard notes, in the surveillant assemblage, 'what differs from the panoptic assemblage is the mechanic architecture,

[148]Kevin Haggerty, 'Tear down the walls: on demolishing the Panopticon' in Lyon (ed), *Theorizing Surveillance: The Panopticon and Beyond* (Willan Publishing 2006) 29.
[149] Brighenti n(106) 62.
[150] Deleuze n(134).

which is now engineered to manipulate data objects in digital networks rather than physical bodies in confined spaces'.[151]

Furthermore, technological growth has enabled the levelling of surveillance undermining and altering traditional hierarchies of visibility. 'Surveillance is not directed exclusively at the poor and dispossessed, but is omnipresent, with people from all segments of the social hierarchy coming under scrutiny'.[152] This includes those groups which were previously exempt from routine surveillance procedures.[153] The technological system which enables the surveillant assemblage allows for the body to be seen outside the traditional form. Indeed, ICT does not focus on the 'individual'. Rather, the focus is on data through which relevant information can be derived. Individuals are therefore broken down into discrete data packets and become 'dividuals'. As Vincent Miller summarises,

> A 'dividual' is not a discrete self, but something which is made up of aggregates of features of discrete selves. Endlessly divided and subdivided, they are a series of features removed from an individual self, placed with aggregates and reconfigured according to various criteria of interest by whatever body has access to the data.[154]

This is indicative of what Bogard calls a 'shift to virtual forms of control' as observation now occurs through the decoding and recording of information.[155] Such a system enables the derivation of meaning from data thereby removing the need for the whole individual; when an individual is targeted by the system for surveillance, it is because of these discrete 'dividual' traits.

---

[151] William Bogard, 'Surveillance assemblages and lines of Flight' in Lyon (ed) *Theorizing Surveillance: The Panopticon and Beyond* (Willan Publishing 2006) 97.
[152] Haggerty n(148) 29.
[153] Haggerty n(146) 606.
[154] Vincent Miller, *The Crisis of Presence in Contemporary Culture* (Sage 2016) Loc 1387.
[155] Bogard n(151) 106

The elements which enable the convergence of social structures into a surveillant assemblage are clearly present in the ICT system which has been discussed in this chapter. The intensification of the capabilities of these technologies results in a radical transformation of the traditional surveillance structures, shifting from a hierarchically situated, unidirectional panopticon, to a levelled system of interconnected nodes of surveillance composed of heterogeneous elements. The proliferation of digitalisation and technology in field of law enforcement has fundamentally changed the role of the police. Such developments therefore require an examination of the impact of the system.

VI. Conclusion

The aim of assessing the impact of the development of the ICT system on the social is to clearly identify norms and values which are impacted by the technology. The transformations of the socio-technical system as a result of technological developments often impose changes upon people and societies without a careful evaluation of the harms and benefits, changes in values, and necessity of the developments.[156] This thesis argues that this has occurred in the development and adoption of the ICT system by the police for investigative purposes. However, there has not been a concomitant development in privacy in line with the changes in values and norms occasioned by these technological developments. The ICT system herein represents the context within which privacy will be assessed using the contextual integrity decision heuristic developed in the preceding chapter. The norms and values identified here are now discussed in the context of the particular element of the system to which they relate: retention, access, and analysis. This discussion will allow for a careful evaluation of the ascribed context relative informational norms and resultant impact on privacy.

[156] Nissenbaum n(44) 161.

CHAPTER 3: COMMUNICATIONS DATA RETENTION

I. Introduction

In order to assess how the use of communications data by law enforcement alters informational norms associated with ICT in a manner that results in a privacy violation, it is necessary to examine the processes within which this information is used. This chapter is the first of three which examines those processes. The focus here is on the collection and retention of communications data. Since the attacks in 2001 there has been an increased focus on terrorism and threats to national security leading to legislative developments in the field of data retention. These laws have become pervasive and expansive. Communications data retention in this regard has become an effective and accepted law enforcement tool in the United Kingdom. This is in part due to the significance of communications data for investigations. 'Communications data has played a significant role in every Security Service counter-terrorism operation over the last decade and has been used as evidence in 95% of all serious organised crime cases handled by the Crown Prosecution Service'.[1] Its retention enables law enforcement to have access to a large quantity of information which it can use to further its investigations making it useful for the prevention, detection, and prosecution of crime.[2] However, this does not mean that data retention represents a legitimate limitation on

[1] Home Office, *Regulation of Investigatory Powers Act Consultation: Acquisition and Disclosure of Communications Data and Retention of Communications Data Codes of Practice* (2014). Noted in this are several examples of cases where this information was used. This included: Operation Frant where telephone evidence of cell site data and call logs revealed participants of a drug ring binging high grade heroin into London; Operation Backfill where internet data was used to identify perpetrators of armed robberies; and Operation Notarise which led to the arrest of over 600 suspected paedophiles. See also: David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (Stationary Office 2015) Annex 10.

[2] Home Office, *Protecting the Public in a Changing Communications Environment* (Cmd 5668, 2009)*:* This was the case in the Rhys Jones murder wherein communications location data showed the suspects at key locations and times; similarly in the Holly Wells and Jessica Chapman murders Ian Huntley's alibi was disproved using mobile phone communications data.

privacy, particularly when its expansive scale and indiscriminate scope are considered.[3] Criticisms of these powers have been accompanied by judicial rulings which refute the legitimacy, necessity, and proportionality of this law enforcement mechanism and result in changes to the legislation.

Data retention is a core function of the ICT system at issue in this thesis. This chapter will be comprised of three parts. Part I will proceed by setting out the elements which enable data retention. Part II will then trace the evolution of data retention in legislation, paying particular attention to the technological advances and social changes which contributed to this evolution. Finally, in Part III, using the contextual integrity decision heuristic set out in Chapter 1, discussion will then turn to whether the changes demonstrated through the development of this component have resulted in a breach of privacy. This is exhibited through an analysis of how the changes in actors, information types, and transmission principles have altered the end values of retention. This analysis will substantiate the argument that data retention as provided for in the investigatory powers instruments breaches contextual integrity and represents a *prima facie* privacy violation.

II. Elements of the system which enable data retention

Before proceeding with further discussion as to its significance, it is instructive to briefly define what is meant by data retention. In this context, data retention is the collection and storage of information generated through telephone and internet usage. The data therein can take several forms but may be classified into two primary categories: content

[3] Ewan MacAskill et al, 'GCHQ taps fibre-optic cables for secret access to world's communications' *The Guardian* (21 June 2013) GCHQ <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> accessed 21 Aug 2015.

data[4] and communications data. The focus is on the latter. Communications data can be separated into three categories: traffic data, location data, and data used to identify the subscriber. In essence, communications data covers all aspects of data except the actual content of the communication; it is the principle artefact of the ICT system at issue in this thesis. This data is generated through the use of services run by providers of public electronic communications networks and/or providers of public electronic communications services.

Retention then, is the storing of all communications and transactions for a set period of time. This time period is longer than the period for which the data would be kept purely for billing and engineering purposes.[5] Retention in this regard is the addition of an obligation on service providers to retain data longer than they would for business purposes, in order to facilitate access by approved agencies. Retention is required by any CSPs who are placed under notice by the Secretary of State when he has deemed it necessary and proportionate to satisfy a number of legitimate aims, including national security and preventing or detecting crime.[6] It is irrelevant if the data is ever accessed; it is merely the possibility that it may be which means retention is required. Further, it encompasses all service users. It is a blanket measure which occurs irrespective of individual suspicion or judicial authorisation. This aspect can be contrasted with the concept of data preservation which typically occurs upon the issuance of a warrant or a subpoena requiring a service provider to keep particular data about a specified individual for a set period of time.

[4] Retention of content is governed by the Investigatory Powers Act 2016 and previously under the Regulation of Investigatory Powers Act 2000. The content of communications is considered more invasive and therefore governed by stricter safeguards including judicial authorisations for interceptions.
[5] Edgar Whitley & Ian Hosein, 'Policy discourse and data retention: The technology politics of surveillance in the United Kingdom' (2005) 29 Telecommunications Policy 857.
[6] The list of reasons a notice can be issued is expansive. The Investigatory Powers Act 2016 s 61(7) lists the reasons obtaining communications data may be deemed necessary.

The data must be retained securely by the CSP by instituting several levels of security to ensure the protection of the data and prevent unauthorised access.[7] This includes access by the company after the period during which the data would have been kept for business purposes. CSPs may receive some compensation for the implementation of these processes, but in practice they absorb the majority of the costs on their own initiative.[8] The notices requiring retention must be kept under review to ensure that they remain necessary and are subject to a formal review every two years.[9] After the review, a determination is made as to whether the retention remains necessary, and therefore the notice is continued; or whether there is need for a variation or revocation of the notice. A variation may occur for several reasons. For example, a CSP launching a new service or generating new categories of data which might be of interest to law enforcement will require an amended notice.[10] Similarly changes in the needs of law enforcement to have access to additional data may require a variation.[11] If retention is no longer required, the notice can be revoked and therefore the CSP will no longer be required to retain the data for any purposes or periods of time outside their ordinary business use.[12]

The communications data retained in the aforementioned manner is the principal artefact of this component of the ICT system. Organisational components in the form of CSPs and legislation interact with this data. Both the organisational and legislative elements have specific aims in retaining the data which lend themselves to different objectives. The legislative aims focus on the value of the retained data for law enforcement and national security. 'Retained data enables the construction of trails of evidence leading up

[7] Home Office, *Retention of Communications Data Code of Practice* (9 December 2014)
[8] Home Office, *Retention n*(7) para 5.2.
[9] Investigatory Powers Act 2016 s 90.
[10] IPA n(9) s 94(1).
[11] IPA n(9) s 94(8).
[12] IPA n(9) s 94(13).

to an offence and they are used to discern, or to corroborate other forms of evidence on the activities and links between suspects'.[13] CSPs on the other hand, retain data to facilitate business functions; any data that does not satisfy this objective is unnecessary. Both the legislative and organisational components play a significant role in the interactions with the artefact, and these interactions define how this element of the overall ICT system is created and utilised. The subsequent section will analyse how these elements interact by tracing the development of data retention through legislation.

III. The evolution of data retention

Data retention has undergone several legislative iterations. The social, political, and technological factors which motivate the development of the legislation play a significant role in its construction and scope. Discourses around retention frame it as a mechanism to increase security without significant downsides; proponents use language to moderate the debate around data retention framing it in non-controversial terms which liken it to nothing more intrusive than a phone bill.[14] However, the changing nature of the data and the retention system challenges this classification. The evolution of the powers of data retention, and the myriad factors which contribute to their development, must be addressed in order to determine how to account for these factors in future legislation. The following traces the evolution of data retention powers in the UK with regard to these relevant factors in order to address how, in this context, privacy is violated by these practices.

[13] European Commission, *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)* (18.4.2011, COM (2011) 225 final, 2011).
[14] Whitley n(5) 860.

a. Data Protection Act 1998 and Privacy and Electronic Communication Regulations 2003

The earliest statutory provisions regarding data retention in the United Kingdom can be found in the Data Protection Act 1998 (DPA) and subsequently in the Privacy and Electronic Communication Regulations 2003 (PECR).[15] It is important to note that this Act *only* covers retention for the private business purposes of companies; it does not provide for retention for law enforcement which is the primary focus of this chapter. However, it is instructive to see how retention is treated in private law and important to note that without the developments of subsequent legislation, this Act, and the 2003 Regulations,[16] would be the primary mechanisms through which the data would be retained. These Acts thereby form the guiding principles which organisations use for private data retention.

These instruments require that data is only retained for as long as necessary for business purposes, after which it must be destroyed or deleted.[17] Data may only be used for legitimate commercial reasons; any other use will give rise to liability.[18] These requirements, along with other core data protection principles,[19] limit the utilisation of data. Retention under the DPA and PECR is thus restricted to the legitimate uses of the company; it is not meant to be accessed by outside parties. The instruments do however,

[15] However, retention did exist in various forms prior the passage of those legislative instruments and in other jurisdictions. For example, Project SHAMROCK in the United States allowed telephone companies to record copies of all international telegraphs entering the United States from 1945 until 1970. Alan Rozenshtein, 'Surveillance Intermediaries' (2017) 70 Stanford L R 1, 133.
[16] As of May 2018, the Data Protection Act 1998 was repealed and replaced by the Data Protection Act 2018 s 44.
[17]Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426 s.5; Data Protection Act 1998 Schedule I Part 1(5).
[18] *Ibid*
[19] The fair information principles set out in Schedule I of the Data Protection Act 1998 require that data: must be fairly and lawfully processed; must only be processed for limited purposes; such processing must be adequate, relevant, and not excessive; the data must be accurate and kept up to date; the data must not be kept for longer than is necessary; the data must be processed in line with a person's rights; the data must be kept secure; and that the data may not be transferred to other countries without adequate supervision.

provide for exemptions to these limitations for national security purposes.[20] Similarly, they provide for exemptions from the information principles of fair and lawful processing and the requirements to inform data subjects when their data has been processed when the data is accessed or processed for legitimate law enforcement purposes.[21]

However, these instruments do not provide for a mandatory retention regime or for the retention of such data for longer than is necessary for ordinary business purposes; it remains at the discretion of the company to retain data subject to the aforementioned limitations. This lack of retention which fulfilled law enforcement and national security aims is classed as the reverse salient of this development; it was a problem identified by the relevant social group necessitating changes to the system. As law enforcement cannot compel the retention of additional categories of data or retention for longer periods to facilitate investigations in these instruments, there is a gap in the capabilities of law enforcement to access relevant data. As communications data became an increasingly practical law enforcement tool due to technological developments, the need for more data retention to allow for more access was recognised, resulting in legislation to require retention by CSPs.

b. Anti-Terrorism Crime and Security Act 2001(ATCSA)

As a result of the capability gap between data retained by CSPs during their ordinary business dealings and data desired by law enforcement, the Anti-Terrorism, Crime, and Security Act (ATCSA) 2001 was enacted, under which a voluntary code was introduced to allow CSPs to retain communications data for periods longer than necessary for

[20] DPA n(16) Art 28; Under this exemption, access can be granted in limited circumstances to data which is retained under these instruments. They cannot compel the retention of additional data or data which is deemed 'more useful' for these purposes. The relevant provisions concerning access to communications data is the subject of Chapter 4.
[21] DPA n(16) Art 29.

business purposes in order to facilitate law enforcement and national security operations. The relevant provisions under the Act stated that the Secretary of State may make a voluntary code of practice relating to the retention of communications data by CSPs and enter into arrangements with these companies in regards to such retention. [22] The primary purpose of enabling retention under ATCSA was to ensure that such data could be retained for later access for the purpose of safeguarding national security or for the prevention or detection of crime or prosecution of offenders which may relate to national security, either directly or indirectly.[23]

This statute represented a move toward a more expansive data retention regime oriented at facilitating law enforcement and national security aims. Its context is particularly important. ATCSA was passed following the events of September 11th and largely in response to those events. Indeed, in its explanatory memorandum, it was noted that: 'The purpose of this Act is to build on legislation in a number of areas to ensure that the Government, in the light of the new situation arising from the September 11 terrorist attacks on New York and Washington, have the necessary powers to counter the threat to the UK'.[24] The motivating factors were a result of increased demands for security to counter these threats; the existing technological capabilities of companies presented an attractive mechanism to enable these aims. However, the voluntary nature of the code of practice and requirement to retain here meant these mechanisms were not as effective as the policy intended. Furthermore, economic concerns were raised over the potential risk of CSPs relocating servers outside of the jurisdiction in order to avoid legal and

[22] Anti-terrorism Crime and Security Act 2001, part 11 s 102. Pursuant to s 103, the code specified periods of retention for relevant categories of data.
[23] ATCSA n(22) s 102(3).
[24] ATCSA n(22).

regulatory requirements arising from any retention obligations.[25] As such, the voluntary nature of the retention under ATCSA was found to be inadequate to meet the needs of law enforcement, resulting in further changes.

c. Directive 2002/58/EC

In addition to domestic legislative developments, there were moves at the EU level to ensure that retention was permitted and harmonised across member states. Much like domestic law, at the EU level retention was first found in general data protection law. Prior to 2002, data retention at the EU level was governed by the General Data Protection Directive 95/46/EC which, like the domestic Data Protection Act, limited data retention to business uses; and Directive 97/66/EC on the protection of privacy and personal information in the telecommunications sector. The latter was meant to complement Directive 95/46 and ensure that fundamental rights were protected in the processing of data. Directive 97/66 provided for the possibility of Member States adopting legislative measures for the protection of public security, defence, or public order when the measures at issue were for the enforcement of criminal law.[26] Directive 97/66 was subsequently amended by Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

The purpose of this Directive was to harmonise provisions of the Member States in order to ensure the confidentiality of communications and related traffic data in national legislation.[27] Directive 2002/58 prohibited the interception and surveillance of

[25] Casper Bowden, 'CCTV for inside your head: blanket traffic data retention and the emergency anti-terrorism legislation' (2002) 8(2) Comp & Telecom L R 21, 22.
[26] 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 (1998) OJ L 24, Art 14(1).
[27] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data in the electronic communications sector (2002) OJ L201, Article 5(1).

communications and related traffic data by persons other than users, unless done with their consent.[28] This provision arguably ensured protection for personal data and communications and prevented indiscriminate access. However, these provisions were qualified by Article 15(1) of the Directive which stated that 'Member States may restrict rights if necessary, appropriate, and proportionate within a democratic society to safeguard national security, defence, public security, the investigation, detection and prosecution of criminal offences, or the unauthorised use of the electronic communication systems'.

The Directive however, was not meant to create a law enforcement mechanism. This was explicitly excluded from its remit.[29] The core aim was to place telecommunications providers on an equal footing and ensure that the data thereby generated was subject to retention. This retention remained limited and only encompassed that data storage deemed necessary for the provision of the telecommunication service or for billing.[30] The capabilities of law enforcement regarding this data remained ambiguous. The provisions regarding the inapplicability of the Directive to law enforcement demonstrated that it wasn't the primary focus of the bill; yet arguably, the provisions set forth were frequently used in a manner that aided law enforcement. However, the limitation on the powers with regard to law enforcement within the Directive meant that it was an ineffective mechanism for ensuring that law enforcement could achieve its objectives in this field.

[28] *Ibid.*
[29] Directive 2002/58/EC n(27) Art 1(3).
[30] *Ibid* Recital 26.

d. Directive 2006/24/EC

In the years following the passage of Directive 2002/58, Europe experienced terrorist attacks, with the Madrid train bombings in 2004 and the 7/7 attacks in London in 2005. These attacks prompted the European Union to extend powers of retention, with the institutions noting that establishing rules on the retention of communications data was a priority, particularly due to its beneficial uses in the investigation and prevention of terrorism and 'serious crime'.[31] These rules took the form of Directive 2006/24/EC, also known as the Data Retention Directive. Stakeholders involved in the passage of the Data Retention Directive noted that given the strong atmosphere of anti-terrorism at the time, there was essentially no resistance offered to the proposed powers, enabling the measure to be passed with ease.[32] Notably, Recital 11 of the Directive acknowledged the significance of data retention for law enforcement:

> Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.

Directive 2006/24 created a substantive regime to legislate for the retention of data. Articles 1(2) and 3(2) detailed the categories of data to be retained. Namely the data necessary for identifying: the source, destination, date, time, duration, and types of a

[31] Whitley n(5) 865.
[32] Monica Horton, *The Closing of the Net* (Polity Press 2016) 59.

communication, and the equipment and location of the equipment used to transmit the data. The Directive also extended to unsuccessful call attempts. However, 'the Directive was careful to note that communication service providers were not required to collect information they do not already collect'.[33] Article 5 covered the periods of retention, requiring Member States to provide for retention for no less than 6 months and no more than 24 months.

Yet despite clearly setting out the role and aim of retaining this data for law enforcement, the Directive was put forward as an internal market measure, with the primary purpose identified as harmonising policies across service providers in order to remove limitations to the market.[34] As justification, the Commission argued that:

> The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation and prosecution of criminal offences presents obstacles to the internal market for electronic communications; service providers are faced with different requirements regarding the types of traffic data to be retained as well as the conditions and periods of retention.[35]

In choosing to classify the Directive as an internal market measure rather than a law enforcement tool, the Commission further argued that previous legal instruments had been based on this legal basis, and therefore subsequent Directives regarding CSPs should as well.[36] However, the overall goal of the Directive was arguably the promotion

[33] Philip Ward, *The Data Retention and Investigatory Powers Bill* (House of Commons Library 14.7.2014, SN/HA/6934, 2014) 6.
[34] To this end, the Directive was enacted under Article 95 TEC (Art 114 TFEU).
[35] Directive 2006/24/EC 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 2005 (2006) OJ L105 Recital 5.
[36] European Commission, S*taff working document - Annex to 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*

of law enforcement rather than harmonisation. Indeed, the goal of harmonisation was to make the data more readily accessible to law enforcement,[37] not for the promotion of any particular economic interest of the CSPs.

The legal basis to the Directive was challenged in the case of *Ireland v the Parliament and the Council* wherein Ireland asked the Court of Justice of the European Union to annul the Directive. Ireland submitted: 'that the sole objective or, at least, the main or predominant objective of that directive is to facilitate the investigation, detection and prosecution of crime, including terrorism'.[38] Therefore, they argued that the Directive should have been adopted under Title IV of the EU Treaty. The Court did not agree. The Court noted that according to recitals 5 and 6, the Commission had acknowledged there were legal and technical disparities in Member States concerning the retention of data and these policies varied greatly imposing extra costs on service providers who were required to enact them.[39] The Court held that, 'In the light of that evidence, it is apparent that the differences between the various national rules adopted on the retention of data relating to electronic communications were liable to have a direct impact on the functioning of the internal market and that it was foreseeable that that impact would become more serious with the passage of time'.[40] The Court further acknowledged that the Directive did not harmonise law enforcement procedures nor in itself permit access to the relevant data.[41] The Court therefore held that the Directive did primarily relate to the functioning of the internal market and dismissed the claim.

---

electronic communication services and amending Directive 2002/58/EC - Extended impact assessment (0438, 2005) 1131.

[37] Directive 2006/24/EC n(35) art 3.

[38] C-301/06 *Ireland v Parliament & Council* [2009] All ER 89 para 28.

[39] *Ireland* n(38) para 66-67.

[40] *Ireland* n(38) para 71.

[41] *Ireland* n(38) para 83.

Under Directive 2006/24/EC it is possible to see the different motivating factors of both the organisational and legislative elements of the system. For CSPs, the lack of harmonisation in policies placed an additional burden on service providers operating in multiple jurisdictions to alter their systems across borders and imposed additional financial costs. Further, differing requirements could place some providers at a competitive advantage over others depending on what the specifics of the domestic retention law required. However, there was also a clear law enforcement objective which guided the passage of this legislation and provided a repository of data for investigative aims. However, despite these motivating factors, the Directive merited criticism. It lacked specifications of the data to be retained and had limited provisions governing any subsequent access to the information. Such issues would be brought to the fore in subsequent legal challenges and lend themselves to the eventual invalidation of the Data Retention Directive.

e. Data Retention (EC Directive) Regulations 2007 and Data Retention (EC Directive) Regulations 2009

Following the enactment of Directive 2006/24, the United Kingdom issued the Data Retention (EC Directive) Regulations 2007 to implement the provisions of the Directive domestically. These regulations covered the retention of data from fixed and mobile line telephony. The Regulations created an obligation to retain data generated in the process of supplying communications for a period of 12 months.[42] The 2007 Regulations did not require CSPs to retain data 'derived from internet access, internet e-mail, or internet telephony'.[43] The UK issued a declaration pursuant to Article 15(3) of Directive 2006/24

[42] The Data Retention (EC Directive) Regulations 2007, SI 2007/2199.
[43] *Ibid* Art 4(5).

that they would postpone provisions regarding internet data retention.[44] These provisions were enacted in the Data Retention (EC Directive) Regulations 2009.

The Data Retention (EC Directive) Regulations 2009 brought fixed and mobile telephony and internet communications under the same legislative umbrella. The principal difference between these regulations and the previous regime was the inclusion of internet, email, and VoIP content (i.e. Skype), even where these data types do not readily translate into the categories listed.[45] The 2009 Regulations must be distinguished however in that they were the first statutory instrument in the UK to *mandate* retention for both telephone and internet data. A positive obligation was imposed on those companies to retain data generated by ordinary purposes beyond what they retained in the normal course of events, solely to facilitate law enforcement activities; failure to do so could result in civil proceedings being initiated by the Secretary of State.[46]

f. Joined Cases C-293/12 and C-549/12 Digital Rights Ireland v Minister for Communication & Ors and Seitlinger & Ors

The 2009 Regulations remained in effect until after the case of *Digital Rights Ireland* which resulted in significant changes to data retention and resulted in legislative amendments. The case occurred as a result of a challenge to Directive 2006/24/EC. Directive 2006/24 was highly criticised for being too expansive in its scope and interfering with fundamental rights. In several Member States, laws implementing the Directive were postponed or overturned due to perceived conflicts with fundamental

[44] This was done to give the Government more time to consider the more complex implementation rules associated with this type of data. Explanatory Memorandum to the Data Retention (EC Directive) Regulations 2007 para 4.1.
[45] The Data Retention (EC Directive) Regulations 2009, SI 2009/859. The DRR 2009 collected new categories of internet data such as email based solely on online servers such as Gmail and encompassed instant messaging capabilities, expanding the scope of internet retention.
[46]DRR 2009 n(45) ss 10(5) – 10(6).

rights.[47] Challenges in domestic courts questioned the compliance of the Directive with the requirements of necessity, proportionality, and foreseeability under relevant human rights instruments. However, the Directive continued to stand until the case of *Digital Rights Ireland* (*DRI*) which challenged the validity of the directive before the Court of Justice of the European Union (CJEU).

The applicants in *Digital Rights Ireland* originally brought a legal challenge before the Irish High Court concerning the direction for telecommunications service providers to retain telecommunications data. The applicant possessed a mobile phone and had used that phone since the provisions regarding retention under Directive 2006/24/EC and the relevant domestic law[48] were enacted. They alleged that the implementing measures instituted by Ireland to ensure compliance with the Directive allowed the named defendants to exercise control over data relating to the plaintiff and other users of mobile phones. Specifically, the applicants argued that the obligation on telecommunications service providers to retain data permitted control of and access to the data in violation of fundamental rights obligations.

The applicant argued that such an order was incompatible with Articles 7, 8, 11 and 41 of the Charter of Fundamental Rights and Article 8 ECHR. In holding to refer the issues to the CJEU, McKechnie J. in the Irish High Court noted:

> Given the rapid advance of current technology it is of great importance to define the legitimate legal limits of modern surveillance techniques used by governments, in particular with regard to telecommunications data

[47] See Decision no 1258 from 8 October 2007 of the Romanian Constitutional Court [Romania]; BVergF, Judgment of the First Senate of 2 March 2010 – 1 BvR 256/08 paras 1-345 [Germany]; Judgment of the Czech Constitutional Court of 22 Mar on Act No 127.2005 and Decree No 485/2005 [Czech Republic].
[48] Criminal Justice (Terrorist Offences) Act 2005 (IRE) Part 7.

> retention; without sufficient legal safeguards the potential for abuse and unwarranted invasion of privacy is obvious. Its effect on persons, without their knowledge or consent, also raises important question indicative of a prima facie interference with all citizens' rights to privacy and communication.[49]

The significance of these developments and the potential for their interference with fundamental rights necessitated further judicial scrutiny. The CJEU examined three principal areas to determine whether the Directive was valid: its compatibility with the right to privacy set out in Article 7 of the Charter and Article 8 ECHR; compatibility with Article 8 of the Charter concerning the protection of personal data; and compatibility with Article 11 of the Charter concerning freedom of expression. In determining whether there had been an interference, the Court took note of the capabilities of communications data, finding that:

> Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of these persons and the social environments frequented by them.[50]

In doing so, the CJEU accepted the extensive nature of communications data and its ability to interfere with individual rights. The CJEU found that such retention policies amounted to an interference, and held that 'the interference with the fundamental rights

[49] *Digital Rights Ireland Ltd v Minister for Communication & Ors* [2010] IEHC 221, para 108.
[50] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications & Ors and Michael Seitlinger & Ors* [2014] 2 All ER para 27.

laid down in Articles 7 and 8 is wide-ranging and it must be considered particularly serious'.[51]

However, an interference, regardless of its seriousness, may be justified if it satisfies the requirements under Article 52 of the Charter, principally that any limitation with the rights laid down in the Charter is in accordance with law, in the general interest, necessary and proportionate. The CJEU found that the provisions regarding retention were in accordance with the relevant national law and accepted that 'the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an object of general interest'.[52] The objective of the fight against 'serious crime' and terrorism was accepted as a legitimate aim:

> As regards the necessity for the retention of data by Directive 2006/24, it must be held that the fight against 'serious crime', in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24.[53]

Yet, in light of the role of personal data and the right to respect for private life, the Court found that the EU's discretion to interfere should be reduced and general review of that discretion should be strict.[54] The failure to circumscribe the retention of data meant that

[51] *DRI* n(50) para 37.
[52] *DRI* n(50)para 44.
[53] *DRI* n(50) para 51.
[54] *DRI* n(50) para 52.

the Directive was not balanced. The Court recognised that data retention could be a valuable tool, acknowledging that it may be appropriate for obtaining objectives relating to criminal investigations,[55] but qualified this observation by noting that data should be limited to that data pertaining to a particular time period, geographic zone, particular circle of people likely to be involved, or of persons whose data would likely to contribute to the prevention, prosecution or detection of offences. The Directive was declared invalid. As a result, domestic laws which implemented the provisions were liable to legal challenges on the basis of the precedent set in *DRI*. This presented a potential obstacle to the mandatory retention systems in the UK enacted under the 2007 and 2009 Data Retention Regulations.

g. Data Retention and Investigatory Powers Act 2014

Following the CJEU ruling in the *Digital Rights Ireland* case the UK passed emergency legislation to ensure that law enforcement could maintain their abilities in order to meet the growing threats of serious organised crime and terrorism.[56] Then Home Secretary, Theresa May, in noting the importance of this legislation, stated that: 'There is no greater duty for a Government than the protection and security of their citizens when we face the very real and serious prospect that the police and intelligence agencies will lose vital capabilities that they need in order to do their jobs'.[57] The legislation now took the form of the Data Retention and Investigatory Powers Act (DRIPA). DRIPA effectively replicated previous previsions on data retention which had been embodied in the Data

[55] *DRI* n(50) para 49.
[56] Ward n(33) 2. Other EU Member States also amended their legislation in the wake of the *Digital Rights Ireland* ruling. In Belgium, data retention is still permitted but strict safeguards and security measures for the data have been added. Slovakia abolished the preventative blanked retention and storage of data and also introduced further safeguards for data. In Hungary, rather than limiting the scope of data retention and implementing stronger safeguards, the opposite occurred. The Hungarian Act requires service providers to store all metadata, including that related to encrypted communications, thereby widening the scope of data retention.
[57] HC Debates col 705, 15 July 2014.

Retention Regulations 2009 and placed the requirement of retention by CSPs into a primary legislative instrument. Specific implementing measures and detailed obligations for CSPs were set forth in the Data Retention Regulations 2014 following the passage of the Act.[58]

Part 1 of this Act replaced the 2009 regulations and reinforced the types of data,[59] matters that may be provided for,[60] periods of retention,[61] and access to data.[62] In determining whether to require a CSP to retain data, the Secretary of State could take a number of factors into account: the size of the CSP, their speed of growth, the number of requests for data typically received by the CSP from law enforcement, whether a CSP operated a specialised service, and whether they operated in a specific area, particularly if they are the sole provider of that service in that particular geographical location.[63] As a safeguard to ensure that data retention was not required indiscriminately, the Secretary of State was also required to consider whether such retention is 'necessary and proportionate' for one or more of the purposes set out under s 22(2) RIPA,[64] which include national security, the purpose of preventing or detecting crime, public safety, and so on.

In assessing the necessity and proportionality of the notice, the Secretary was required to consider a number of criteria. First, she must consider the likely benefit of the notice;[65] a strong case would be made for the retention of categories of data which are known to be of considerable use to law enforcement. Second, the likely number of users who will be affected must be considered.[66] A large customer base increases the volume of data and

[58] Data Retention Regulations 2014, SI 2014/2042.
[59] Data Retention and Investigatory Powers Act 2014 (DRIPA) s1(1).
[60]DRIPA n(59) s 1(4).
[61] DRIPA n(59) s1(5).
[62] DRIPA n(59) s1(6).
[63] Home Office, *Retention* n(7) s 3.3.
[64] DRIPA n(59) 2014 s1(1)
[65] Home Office, *Retention* n(7)
[66] *Ibid.*

its potential usefulness for law enforcement. However, it also represents a greater intrusion. These two competing interests must be balanced. Further, the technical feasibility and cost to the CSP needed to be contemplated.[67] The requirements should be affordable and represent value for money in terms of benefits received without placing an undue burden on the CSP. Finally, the Secretary of State had to take into account what data was required and for how long and assess whether such retention was necessary for the stated purpose. If, on balance, the Secretary of State found that the cumulative effect of these considerations was that retention was necessary and proportionate to the legitimate aims, she could proceed with the process.

If it was provisionally decided that the data must be retained, the Secretary of State would then ideally consult with the CSP, during which the CSP could voice any concerns with the required retention.[68] However, there were no rights of redress for a service provider who believed a notice to retain was disproportionate or requested the cancellation of a notice.[69] Furthermore, at times this consultation process would not be possible, for example when a new technology was released with short notice or there was a new threat that required greater retention. Following the consultation, the Secretary of State communicated the decision regarding the retention of relevant data by issuing a notice to the CSP. The CSP was then required to begin retaining data without undue delay.

DRIPA demonstrates how the relevant social group composed of law enforcement and politicians solved a potential problem in the retention system so that it met their objectives. The ruling in *DRI* meant that retention may no longer be permitted and

[67] *Ibid.*
[68] *Ibid* s 3.9
[69] DRIPA n(59) s 1.

therefore they would lose access to a resource they considered valuable. They utilised the legislative process to ensure that they were able to maintain data retention capabilities. Other elements which interacted with the primary artefact of communications data were similarly affected by this shift but their interests were arguably not represented to the same degree. For example, the organisational elements embodied in CSPs were able to voice concerns with the obligations being placed on them, but there is no indication that these concerns were able to supersede the dominant interest of law enforcement and the State in retaining the data. Further, individual users were also impacted by the retention of their data and the potential interference with privacy that resulted, but they were not effectively represented in the development of this iteration of the retention component.

h. Counter-Terrorism and Security Act 2015

Following the enactment of DRIPA, the Government passed the Counter Terrorism and Security Act (CTSA) 2015, section 17 which altered the data retention regime in two substantive ways. First, the CTSA imposed an obligation on CSPs to retain data which was not already generated or processed in the course of their normal business operations. The CTSA imposed this requirement 'by mandating certain types of communications data that companies must generate and store, regardless of whether this is data which is usually retained for business purposes'.[70] This provision placed a positive obligation on companies to create and maintain facilities for data storage for broad categories of data. CSPs became de facto databases for relevant data for law enforcement and intelligence agencies. Second, CTSA changed the definition of internet data to any communications

[70] Liberty, *Response to the Home Office Consultation on the Acquisition and Disclosure of Communications Data and the Retention of Communications Data Codes of Practice* (Liberty Jan 2015).

data which: related to an internet access service or an internet communications service, or may be used to identify or assist in identifying which IP address or other identifier belongs to the sender or recipient of a communication.[71] This meant that the CTSA aimed to enable law enforcement to link specific devices and accounts to users, even when the equipment or accounts were not specifically registered to that individual. As Liberty recognised:

> The information required to be retained is defined very loosely, even extending to information linking an individual not to an IP address but to any 'other identifier', such as an email address or social media account handle. This provides the opportunity to link different online accounts and internet usage with one device or individual.[72]

The CTSA thereby expanded the retention policies and the utilisation of communications data.

Theresa May acknowledged that the primary aim of the retention requirements set out in this Act was to assist law enforcement.

> Companies generally have no business purpose for keeping a log of who used each address at a given point in time, which means that it is not possible for law enforcement agencies to identify who sent or received a message. The provisions will allow us to require key UK companies to retain the necessary information to enable them to identify the users of their

[71] Counter-Terrorism and Security Act (CTSA) 2015.
[72] Liberty n(70) 12.

> services. That will provide vital additional capabilities to law enforcement in investigating a broad range of 'serious crime', including terrorism.[73]

The overall development of the data retention regime in CTSA demonstrates a distinctive shift in policy toward blanket retention and more expansive categories of data; a shift that the Government argued was necessary for the protection of the public interest in the investigation, detection, and prosecution of crime and the fight against terrorism. The requirements of CTSA, particularly with regards to the change in the definition of internet data, are a result of shifting social elements precipitated by technological development. People possess multiple devices and use separate devices depending on the context. One might use a mobile phone for work and another for home; the one for personal use will likely possess subscriber information directly linkable to the owner whereas the one for work may be owned more generally by the company without any personally identifying information linked to the account. The provisions in CTSA recognise this type of situation and legislate for it so that additional information can be retained so as not to diminish the abilities of law enforcement.

i. Investigatory Powers Act 2016

The current statute regarding communications data retention in the UK is the Investigatory Powers Act 2016 (IPA). The IPA arose due to the sunset clause which was attached to DRIPA which placed its expiration on the 31st December 2016. There was no legal challenge nor radical technological development that precipitated the passage of the IPA at the time it was passed.[74]

[73]HC Debates vol 589, col 214 2 Dec 2014.
[74] It is worth noting here that judicial challenges had been issued against DRIPA but had not been ruled upon at the time of drafting the IPA. The judgment of *Tele2 and Watson* (discussed in the following section) was one such challenge and has implications for data retention in the future.

As it stands, the IPA replicates the previous retention measures which dictate the categories of data with the notable addition of the retention of Internet Connection Records (ICRs). ICRs are communications data which records which internet services a device connects to.[75] These records may establish which websites, applications, messengers, or other internet services are used; when they are used; how they are being used (i.e. mobile phone or other device); and be able to link a specific device to an online communications service.[76] This additional category of data is not one which is retained by CSPs for business uses, nor do they have any reason for doing so. The principal function of this type of retention is to benefit law enforcement. The Home Office stated this in their operational case concerning ICRs,

> Rapid technological change means that law enforcement's inability to access online CD is significant and will only get worse if it continues to be impossible to require communications companies to retain ICRs. More and more communications are taking place over the internet and as this happens it follows that an increasing proportion of CD will be unavailable when it is needed.[77]

Therefore the inability to retain ICRs was seen as a problem which needed to be addressed in the development of the system; it was done so to effectively incorporate the aims of law enforcement.

In order for retention to occur, CSPs must be served with a retention notice. Notably, under the IPA, a retention notice, and any associated requirements or restrictions which result, may relate to conduct and persons outside of the United Kingdom.[78] This includes

[75] Investigatory Powers Act (IPA) 2016 s 62.
[76] *Ibid*
[77] Home Office, *Operational Case for the Retention of Internet Connection Records* (4 November 2015).
[78] IPA n(75) s 97(1).

the positive duty on CSPs who are issued with a notice to comply with the provisions contained therein.[79] This means that the powers contained in the IPA may be applied to non-UK operators and require those operators to take action to give effect to a notice. Such a legislative development represents a significant expansion of jurisdiction beyond the borders of the UK. Companies who provide a service to individuals in the UK can be subject to retention requirements. Much like the process under DRIPA, the Secretary of State must determine that the serving of such a notice meets the threshold for necessity and proportionality.

In assessing the need for a notice, the Home Secretary should take steps to consult with the CSP. In this process the company may request the assistance of the Technical Advisory Board (TAB).[80] The Board is composed of members from both industry and Government and is meant to be an impartial mechanism to consider the impact of a notice and offer advice.[81] However, the validity of the TAB is undermined by several practical limitations. First and foremost, there is no requirement that the Home Secretary amend, vary, or revoke if the TAB determines that it would not be in the CSPs interest to be served with a notice. The TAB's role is solely advisory and their advice and guidance does not have to be followed. Furthermore, the efficacy of the TAB can be undermined by the limitations of the Board itself. The TAB meets infrequently; as of February 2017, the TAB had yet to meet since the IPA received royal assent in 2016.[82] The impartiality of the chair can also be called in to question. Despite Regulations requiring that the chair

[79] IPA n(75) s 95(1).
[80] RIPA s 12(5). The TAB is an advisory panel which provides advice on the obligations placed on CSPs are reasonable [Technical Advisory Board, *Annual Report* (2014-2015) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/477901/Technical_Advisory_Board_Annual_Report_2014-15.pdf> accessed 17 Dec 2017 1.1]
[81] Investigatory Powers (Review of Notices and Technical Advisory Board) Regulations 2018, SI 2018/354. See also: HL Deb vol 788, col 1710, 1 February 2018.
[82] Written Question by Lord Paddick HL5532; In the period of 2014-2015 prior to the passage of the IPA but following DRIPA, the TAB also did not meet.

not serve the interest of either CSPs or law enforcement and national security agencies, the current chair Jonathan Hoyle previously worked as DG of Information Security and Assurance at GCHQ before moving on to the private sector.[83] This does not in itself demonstrate any bias with the board, however, it can create the appearance of unfairness and call in to question the reasoning which underpins the advisory decisions.

Whilst the TAB does not represent an effective and impartial resource in the evaluation of retention notices, the IPA did institute an oversight procedure which aims to improve the legitimacy of the process. Under the IPA, the decision to issue a notice to retain data must be approved by a Judicial Commissioner.[84] In deciding whether to approve the Home Secretary's decision to give a notice, the Commissioner must apply the same principles as would be applied by a court on an application for judicial review and have due regard for privacy.[85] Where the Judicial Commissioner refuses to approve the notice, the matter may be referred to the Investigatory Powers Commissioner. The full powers of the Investigatory Powers Commissioner (IPC) will be addressed in Chapter 6, however, it is important to note here that a refusal by the IPC precludes the issuance of a notice to a CSP. The institution of a process of independent administrative approval for notices does demonstrate a significant development in the overall safeguards for data under the IPA. However, as will be addressed in Chapter 6, this remains insufficient to ensure an effective protection of privacy.

[83] Hoyle was appointed in 1 April 2015 (Technical Advisory Board n(80) 3). Prior to his appointment he had left GCHQ and taken up a post at Lockheed Martin. It is also important to note that this is the most current appointment information as of July 2018. It is unclear whether Hoyle remains chair of the TAB as no further updates have been issued on the role since 2015. Furthermore, no annual reports have been issued for the Technical Advisory Board since the 2014-2015 report.
[84] IPA n(75) s 87(1)(b).
[85] IPA n(75) s 89(2).

j. Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson & Ors

The final element to be considered in the evolution of data retention in the ICT system is the *Tele2* case. This case challenged, among other things, the obligations relating to the general and indiscriminate retention of traffic and location data under DRIPA and their conformity with EU precedent. The case was not decided until after the passage of the IPA; however, as many of the provisions from DRIPA were replicated in IPA it is worth examining the case. There were two conjoined cases at issue here. The first was the Swedish case of *Tele2* wherein a CSP stopped retaining data pursuant to the ruling in *DRI*; they were then informed that they were in breach of national legislation and ordered to recommence data retention. The applicant alleged that the obligation to retain data was a breach of fundamental rights guaranteed by the Charter. The question referred to the court was whether a 'general obligation to retain traffic data covering all persons, all means of electronic communication, and all traffic data without any distinctions, limitations, or exceptions for the purposes of combating crime, was compatible with Art 15(1) Directive 2002/58/EC, taking into consideration Articles 7, 8, and 52(1) of the Charter?'.[86] If not, could retention be permitted where access was limited, data protection and security were provided for, and data was only retained for six months and then subject to deletion.[87]

Like the proceedings in *Tele2*, *Watson & Ors* alleged that the retention was incompatible with Articles 7 and 8 of the Charter and Article 8 ECHR. The High Court held that the judgment in *DRI* had established that legislation which imposed 'a general body of rules

[86] *Joined Cases C-203/15 Tele2 v Post-och telestyrelsen & C-698/15 Watson & Ors v Secretary of State for the Home Department* (2016) ECLI 970 para 51(1).
[87] *Tele2* n(86) para 51.

for the retention of communications data is in breach of the rights guaranteed by Articles 7 and 8 of the Charter, unless that legislation is complemented by a body of rules for access to the data, defined by national law, which provide sufficient safeguards to protect those rights'.[88] The judgment was challenged and the Court of Appeal referred the matter to the CJEU for a preliminary ruling.

In considering the issues, the CJEU noted the broad scope of the legislation and the expansive nature of the information retained.[89] The Court acknowledged the ability of the information to allow 'conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them'.[90] As a result, the Court held that the interference with fundamental rights was considered particularly serious.

The Court had to determine whether this interference could then be justified. The CJEU held that the seriousness of the interference could only be justified for the purposes of fighting crime where it was used the fight *'serious crime'*, and in particular, organised crime and terrorism.[91] Blanket and indiscriminate retention could not be justified. Further, the Court went on to discuss the comprehensiveness of who was potentially caught by the retention provisions noting it 'applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences'.[92] Nor were there any restrictions on the data

[88] *Tele2* n(86) para 53; the requirements regarding access and safeguards are addressed in Chapters 4 and 6 of this thesis respectively so they will not be addressed in detail here.
[89] *Tele2* n(86) para 97 and 98.
[90] *Tele2* n(86) para 99.
[91] *Tele2* n(86) para 103.
[92] *Tele2* n(86) para 105.

in relation to location, time, or persons likely to be involved in 'serious crime'. Therefore, the Court found the retention exceeded what was strictly necessary and the interference could not be justified.

In the implementation of the CJEU ruling, the Court of Appeal granted declaratory relief, holding that s 1 DRIPA was inconsistent with EU law to the extent it allowed access to retained data where the objective was not limited to 'serious crime' nor subject to prior review by an administrative authority.[93] The ruling was confined to the context of the prevention, detection, and prosecution of criminal offences.[94] Notably, the ruling referred specifically to the access requirement, not the retention of data itself. Indeed, in the judgment, Lord Lloyd Jones, specifically addressed whether the ruling in *Tele 2 and Watson* was intended to require retention only for serious criminal offences. In holding it did not, he accepted the conclusion of the Divisional Court that the CJEU 'cannot have meant that [CSPs] can only lawfully be required to retain the communications data of "suspects or persons whose data would contribute to the prevention, detection, or prosecution of serious criminal offences" as such a restriction would be wholly impracticable'.[95] However, this does not sit well with the text of the CJEU judgment in *Tele2 & Watson* which specifically discussed the need for limitations on the retention component of the system.

The subsequent case of *Liberty v SSHD* concerned the compatibility of the IPA with the ECHR and EU law following *Watson* and its application by the Court of Appeal. In this case the claimants asked the Court to make an 'order of disapplication' in respect of Part 4 IPA on the retention of communications data. In so doing, the claimants submitted that

[93] *Watson v SSHD* [2018] EWCA Civ 70 para 27.
[94] *Watson* n(93) para 13.
[95] *Watson* n(93) para 26.

the blanket retention of communications data was incompatible with EU law as it provides for general and indiscriminate retention.[96] The Court disagreed and accepted that the current statutory regime governing retention was sufficient to ensure that the retention was necessary and proportionate.[97] The claimants further submitted that the retention did not meet the necessary 'seriousness' threshold required following *Tele2 and Watson*. The High Court here agreed with the Court of Appeal's reasoning in the implementation of *Watson* and found that the absence of a requirement for 'serious crime' did not invalidate the IPA's provisions regarding retention.

The failure to apply the CJEU's ruling to the retention components arguably goes against the text of that judgment. The focus on access rather than the process of retention itself fails to take into account the reasoning of the CJEU on the blanket and indiscriminate nature of the provisions which represents a serious interference with fundamental rights. However, like the Court of Appeal in *Watson,* the High Court in *Liberty* did agree that the absence of a 'serious crime' requirement and prior judicial review for access meant the IPA was incompatible with EU law. The significance of these rulings in the context of access will be discussed in Chapter 4.

The legal challenges to the data retention regime indicate the contentious nature of these powers. Whilst useful to law enforcement, the wide scope and the scale at which the data is collected and retained raises concerns for individuals and society. It is therefore necessary to look to the shifts in informational norms occasioned by the development of retention capabilities to determine the impact on privacy.

[96] *Liberty v SSHD* [2018] EWHC 976 para 120.
[97] *Liberty* n(96) para 124.

IV. Applying Contextual Integrity to Data Retention

Having established how data retention in the ICT system has evolved, the contextual integrity heuristic set out in the Chapter 1 will now be applied to determine whether these developments have shifted informational norms in a manner which interferes with privacy. Jurisprudence in the field of data retention has accepted that the mere retention and collection of the data triggers a privacy interest.[98] This privacy interest exists irrespective of whether the data is subsequently used.[99] As technologies generate increasing amounts of data and enable the collection and retention of that data at scale, the threat to privacy becomes more significant. The question is not, however, whether a privacy interest is triggered by this retention, but whether privacy is interfered with in an unjustifiable manner. The contextual integrity decision heuristic allows for an analysis of this by looking at the various elements which have been altered as a result of the development of the data retention regime and whether those changes have fundamentally altered normative expectations in a manner that requires subsequent action. In order to determine this, the following section establishes that the extant actors, information types, and transmission principles in the data retention process have been altered as a result of technological developments. Consequently, prescriptive measures are required to ensure that the retention process comports with social norms and future technological developments.

[98] See: *Amann v Switzerland* App no 27798/95 (ECtHR, 16 Feb 2000); *Weber & Saravia v Germany* App no 54394/00 (ECtHR, 29 June 2006) and *Liberty & Ors v GCHQ & Ors* (2014) UKIPTrib 13_77-H 5 Dec 2014; *Leander v Sweden* App no 9248/81 (ECtHR, 26 Mar 1987).
[99] *S and Marper v United Kingdom* App No 30562/04 and 30566/04 (ECtHR, 4 Dec 2008) 121.

In determining whether an informational norm has shifted in a manner that breaches contextual integrity, it is important to consider the context in which the change has occurred. As Nissenbaum notes,

> The nature of alterations varies across systems and practices as each affect, in different ways, the range of recipients, the types of information, and conditions under which information is transmitted from one party to another. Whether the alterations amount to transgressions, and whether these transgressions are morally and politically legitimate depends, of course, on the contexts in which they transpire and how they bear on relevant ends and purposes.[100]

Shifts in information types, transmission principles, and actors must be evaluated within the context of the retention component of the system.

Information types have changed; the evolution of the data retention legislation demonstrates a need to retain greater categories and quantities of data than before. Within this data, the nature and attributes of the retention has changed. This is particularly evident in the increased collection of internet data. The infrastructure which provides access online does not require data retention in the same way as traditional telecommunications.[101] While some of the categories of data can be comparable to their analogue counterparts (i.e. emails instead of letters, VoIP instead of phone calls), new categories of information are also being generated as a result of the provision of different services (i.e. geo-location data which is generated through the use of cell phones). The categories of data to be retained are defined loosely.[102] As a result, the developments in

[100] Helen Nissenbaum, *Privacy in Context* (Stanford University Press 2010) 195.
[101]Matthew Hare's submission to: House of Commons, 'Investigatory Powers Bill: Technology Issues' (HC573 2015).
[102] Liberty, *Response to the Government's consultation on the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data* (18 Jan 2018) <

categories of communications data which have occurred throughout the evolution of retention law have altered the nature of the information. It is no longer basic data concerning a limited suspect pool. It has become a database of the communications of the masses; no distinctions are made between those whom law enforcement has a reason to investigation and those passive users of communications services. Law enforcement sees the increase in the information and the development in its attributes as a valuable tool for investigators. 'As communications technologies have advanced and diversified, the pool of evidence potentially available to investigators has grown – and so has the Government's desire to access it'.[103]

In introducing the Investigatory Powers Bill in 2015, then Home Secretary, Theresa May noted the significance of expanding the categories of data for achieving law enforcement aims. Drawing particular attention to the capabilities that existed for mobile phone information but not for the same type of information generated by non-traditional methods, such as social media or communications apps, May put forth the argument that new categories of data must be retained.[104] While such a method may satisfy a legitimate aim for law enforcement, there is also a normative impact which occurs from categorising data as potentially valuable. Tarleton Gillespie explains that '[c]ategorisation is a powerful semantic and political intervention: what the categories are, what belongs in a category, and who decides how to implement these categories in practice, are all powerful assertions about how things are and are supposed to be'.[105] The

https://www.libertyhumanrights.org.uk/sites/default/files/2018.01.18%20liberty%20consultation%20response%20FINAL.pdf> accessed 4 Feb 2018 12.

[103]Clive Walker C, 'Data retention in the UK: Pragmatic and proportionate, or a step too far?' (2009) 25 Computer Law & Security Review 325.

[104] HC Debates vol 587 col 970, 4 November 2015.

[105] Tarleton Gillespie, 'The Relevance of Algorithms' in Gillespie Boczkowski and Foot (eds) *Media Technologies: Essays on Communication, Materiality, and Society* (MIT Press 2014) 167, 171.

impact of the changes and increases in types of information must be assessed with respect to the norms they embody and the values they promote.

In addition, the transmission principles associated with private retention have been transformed. The negotiated relationships between individuals and companies have been altered. There are now more ways to communicate as people no longer utilise the same CSP for all their services; companies no longer need to keep as much information about their customers, mainly as a result of companies providing fixed rate tariffs rather than billing on individual usage (i.e. charging per minute or per text); anonymization is increasing whereby people no longer use directly attributable personal information when signing up for services; more and more services are based abroad; and communications data is increasingly fragmented as it is sent across multiple platforms using various devices.[106]

Actors in the form of CSPs reflect these changing capabilities and attitudes by expanding their functions. Traditionally, companies were passive intermediaries, connecting two parties. 'Historically, members of our society have taken for granted that we know more about our lives than any third party could, and this knowledge has been vital to our sense of ourselves'.[107] However, increasingly everything that individuals undertake in their everyday lives involves some form of communication and consequently there is little that remains unknowable by the companies which collect and process this information. Despite this shift, the treatment of CSPs has remained static in the legislation. This means that outdated informational norms are being applied to new technologies. Finally, the retention systems themselves have become an important element in the investigative

[106] Home Office, *Protecting* n(2).
[107] Jonah Bossewitch & Aram Sinnreich, 'The end of forgetting: strategic agency beyond the panopticon' (2012) 15(2) New Media & Society 224.

process. These systems are not only access points, but they are the predominant sources of information. As long as these retention systems serve a critical function as a repository of information for law enforcement, privacy interests will be triggered. This indicates that there has been a fundamental shift in the role of CSPs in the retention process, moving it from private actor to public authority. This shift has altered the informational norms and consequently resulted in a breach of contextual integrity.

V. Conclusion

The foregoing analysis demonstrates the evolution of the retention component of the ICT system for communications data. The development of this element shows that the roles of key actors have been altered, information types expanded, and transmission principles altered. The developments here can therefore be classed as a privacy violation using the contextual integrity framework. This violation must be accounted for in any proposed changes to address the privacy issues triggered by data retention. As Ian Brown notes, 'Given the rapid advance of current technology it is of great importance to define the legitimate legal limits of modern surveillance techniques, in particular with regard to telecommunications data retention; without sufficient legal safeguards, the potential for abuse and unwarranted invasion of privacy is obvious'.[108] Retention clearly triggers privacy violations; however, it is not the sole component of the system which results in such intrusions. The following chapter looks to the access element of the ICT system and considers privacy therein.

[108] Ian Brown, 'Communications Data Retention in an Evolving Internet' (2010) 19(2) International Journal of Law and Information Technology, 103.

CHAPTER 4: ACCESS TO COMMUNICATIONS DATA

I. Introduction

The data retention discussed in Chapter 3 provides the repository of information on which subsequent access and analysis is based. Access and analysis interact with the retention component by utilising data that is retained and processing it in a manner that allows for law enforcement to achieve its stated objectives of investigating, detecting, and preventing crime. The focus of this chapter will be on the access element, specifically, who can access the information and for what purposes. The ability to access communications data is not a new power. Historically, investigators would acquire required information through an application to the service provider who could choose to disclose the data. The information sought was that retained by the company for billing purposes. Changes in technology created issues with this process. As David Anderson noted in his review of investigatory powers, 'Proliferating methods of communication, the fragmentation of providers, difficulties in attributing communications, changing business models, and increasing use of overseas service providers have all tended to make data more difficult to access'.[1] Technology in this regard limited the capabilities of law enforcement to access relevant data. Concurrently, technological developments in communications data enabled it to become more expansive, in both the actions it covers and the time periods available. This increased the potential value of the data for law enforcement in investigating not only 'serious crime' but, as the Police Service of Northern Ireland noted, 'an essential tool in investigating even the minor volume crimes that are key indicators of police performance and public confidence'.[2]

[1] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (Stationary Office 2015) 7.53.
[2] Anderson n(1) 7.53.

As demonstrated in the following, as more information is generated through individuals using technologies, the desire of law enforcement to access this information simultaneously increases. These requests are incorporated into the legislation without an adequate assessment of how they will impact on privacy. The passage of such legislation is typically justified by noting that law enforcement agencies are bound by relevant human rights principles when they access the data and they cannot contravene these obligations. Further, communications data is treated as secondary information, less intrusive than content, and therefore the regimes are more permissive and the oversight less rigid.[3] However, such an assessment fails to take into account the nature of the data and the limitations of extant protections for individuals when it is accessed.

To determine the extent to which access to communications data, as dictated by the legal and policy regimes, constitutes an interference with privacy which is not responsive to the nature of the technology and consequently impacts on informational norms, the analysis will proceed as follows. Part I establishes the key elements of the ICT system which enable access to communications data by law enforcement. Part II then assesses how these elements have evolved following technological advances and social changes. Finally, in Part III discussion will turn to how the changes to these methods and processes have violated contextual integrity thereby resulting in a disproportionate privacy violation which cannot be reconciled with the values of the system.

[3] Ian Brown, 'Communications Data Retention in an Evolving Internet' (2010) 19(2) International Journal of Law and Information Technology 102.

II. Elements of the system which enable access to data

Retention and access are inextricably linked as data is only retained for the purpose of making that data later accessible, in this context, by law enforcement.[4] The principal artefacts at issue remain the retention system and communications data which is collected and kept on that system. The organisational component, in the form of CSPs, acts as a facilitator in the access element. CSPs collect and store the information; they are also responsible for its generation through the technologies used by their customers. Legislation seeks to expand the role of CSPs in this regard by requiring the creation of new access capabilities by these private actors. The resultant data pool then becomes the primary focus of law enforcement and consequently a legislative target. The latter seeks to ensure that the data will be readily available for law enforcement by instituting legal regimes which both require retention and provide for access. In this way, law enforcement and the legislature act as system builders, shaping the environment by requiring CSPs to build infrastructure which they can utilise.[5] This is in turn coupled with technological developments which increase efficiency,[6] and allow for information to be extracted which goes far beyond what would accessible to the unaided senses.[7]

[4] *Joined Cases C-203/15 Tele2 v Post-och telestyrelsen & C-698/15 Watson & Ors v Secretary of State for the Home Department* (2016) ECLI 970 para 79.
[5] Donald MacKenzie, 'Missile Accuracy: A Case Study in the Social Processes of Technological Change' in Bijker Hughes and Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012) 208.
[6] Helen Nissenbaum *Privacy in Context* (Stanford University Press 2010) 56 discusses the development and 'datafication' of information which occurs when traditional paper records are transferred to computerised databases thereby making them more efficient and allowing for more to be revealed.
[7] Ben Bowling et al, 'Crime Control Technologies: Towards an Analytical Framework and Research Agenda' in Brownsword and Yeung (eds) *Regulating Technologies* (Hart 2008) 62.

III. The evolution of access to communications data

The elements of the system are considered through an analysis of the evolution of the access requirements for communications data by law enforcement. In doing so, it is necessary to establish the factors which led to legislative changes, including technological advances that increased desired data pools, and changes in social and policy aims which increased law enforcement powers.

a. The Post Office and the case of Malone v United Kingdom

Despite the lack of centralised computer databases of information which exist today, data concerning the who, where, how, and when of communications was historically accessible to law enforcement. What was lacking was any legal underpinning for the access. The historical approach to acquiring this data occurred through a process known as metering. In this, a device known as a 'meter check printer' was attached to a private subscriber's telephone by the Post Office.[8] This printer was used for business purposes, such as ensuring billing was correct, investigating issues with quality, and checking against possible misuse of the phone system. The information collected showed the numbers dialled and the duration of calls, but not what was said.[9] The 'meter check printer' produced a printed tape which contained the information and could be accessed by the police. There were no statutory provisions concerning how the police could access the metered information; it occurred through negotiated discussions with the relevant service providers. During a brief discussion on the practice in the House of

[8] What is now British Telecommunications, as a result of the British Telecommunications Act 1981, which divided the Post Office into two corporations: the Post Office which was responsible for mail, and British Telecommunications, which was responsible for telephones.
[9] Home Secretary Merlyn Rees in HC Debates vol 947, cols 476-7 W 13 April 1978.

Commons in the 1970s, the Home Secretary at the time, Merlyn Rees, noted that the information may be provided if:

> The information is vital to police inquiries in a matter of 'serious crime', and cannot be obtained from any other sources, or where the police are investigating calls made by fraudulent methods with intent to avoid due payment to the Post Office, or offences under Section 78 of the Post Office Act 1969 – which includes, for example, indecency, menacing, and annoyance.[10]

The process of metering was challenged in the case of *Malone v United Kingdom.* The case concerned the interception of Mr Malone's telephone conversations. Malone alleged that at the request of the police, his correspondence had been intercepted and his telephone had been tapped and metered in breach of his Article 8 and 13 rights under the ECHR.[11] On the issue of interception, the ECtHR held that there was an interference by a public authority with the right guaranteed in Article 8(1) ECHR. The Court considered whether that interference could be justified 'in accordance with law' for a recognised purpose 'necessary in a democratic society'. In holding that the provision was not in accordance with law, the Court noted that the procedures 'did not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on public authorities'.[12] Therefore, the necessary minimum degree of protection for citizens under the rule of law was lacking. As the interception was found not 'in accordance with law', the Court did not consider it necessary to examine whether the interference met the requirement of being 'necessary in a democratic society'.[13]

[10] Home Secretary Merlyn Rees in HC Debates vol 944, cols 760-1W 23rd Feb 1978.
[11] *Malone v United Kingdom* App No 8691/79 (ECtHR, 2 Aug 1984).
[12] *Malone* n(11) para 79.
[13] *Malone* n(11) para 81.

As regards the metering, the Court noted that metering must be distinguished by its very nature from interception. The Court acknowledged the fact that the meter is legitimately provided by the telephone service provider and is used for commercial reasons. The Court held that the private interest in metering meant it should 'be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified'.[14] This interpretation implies that the Court saw the collection and potential release of communications data as a socially acceptable practice, in contrast with the interference with intercepted content. However, that does not mean that the data collected from this metering cannot result in an interference with Article 8. Indeed the Court held that: 'The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, the release of that information without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8'.[15] In determining whether this was 'in accordance with law' the Court noted that s 80 of the Post Office Act 1969 allowed for the provision of information to persons holding office under the crown, but they were not required to disclose this information.[16] The primary guiding principles for when this information should be provided were simply set out in answers to parliamentary questions. However, the Court found that there were no

[14] *Malone* n(11) para 84. This line of thought is largely reflected in the development of legislation surrounding communications data. The idea that the data is generated from private functions is put forward as one of the principal arguments as to why law enforcement should not be seen as interfering with privacy rights when utilising that data. The argument that it is socially acceptable to examine this data but not data that is directly intercepted by law enforcement is tenuous at best and a distinction that cannot hold in light of technological developments as will be demonstrated throughout this thesis.

[15] *Malone* n(11) para 84.

[16] Post Office Act 1969 s 80 states: A requirement to do what is necessary to inform designated persons holding office under the Crown concerning matters and things transmitted or in the course of transmission by means of postal or telecommunication services provided by the Post Office may be laid on the Post Office for the like purposes and in the like manner as, at the passing of this Act, a requirement may be laid on the Postmaster General to do what is necessary to inform such persons concerning matters and things transmitted or in the course of transmission by means of such services provided by him.

legal rules concerning the scope and manner of exercise and discretion of public authorities and therefore the practice was not 'in accordance with law'.

While not substantially discussed in the main judgment, it is worth noting the concurring opinion of Judge Pettiti who recognised the potential intrusiveness of metering data. Judge Pettiti noted the comprehensive nature of the data obtained regarding telephone communications, including their origin, destination, and duration, and noted that 'when effected for a purpose other than its sole accounting purpose, albeit in the absence of any such interception as such, [the metering] constitutes an interference in private life'.[17] Regardless of the fact that the service provider had an interest in obtaining the data, the fact that it could then be used for other purposes was enough for it to be classed as an interference with private life. Judge Pettiti further noted how the nature of the data enhanced the abilities of law enforcement. 'On the basis of the data thereby obtained, the authorities are enabled to deduce information that is not properly meant to be within their knowledge'.[18] Despite occurring before the widespread use of computerised databases and technological developments such as the internet, Judge Pettiti's concurring opinion sets out two key issues regarding communications data which remain relevant to this day: the role of the private actors who generate and possess the data, and the ability of law enforcement to make inferences and judgments based on the data. Even as early as *Malone* it was recognised that the nature of the data and the role of private actors were factors in determining whether interference with this information represented a violation. However, much of the subsequent legislation fails to take this into consideration.

Following *Malone,* the Interception of Communications Act 1985 was enacted. This statute provided for the process of interception of communications following the issuance

[17] *Malone* n(11) concurring judgment of Pettiti.
[18] *Ibid*

of a warrant when the Secretary of State considers it necessary for limited purposes such as national security or preventing or detecting 'serious crime'. There was no explicit discussion of information such as that obtained by metering in the Act and the practice remained unregulated. As such, access to communications data by law enforcement remained outside legislative mechanisms until the Regulation of Investigatory Powers Act 2000.

b. Regulation of Investigatory Powers Act 2000

Prior to 2000, the only provisions concerning the access of communications data by law enforcement were found in the Data Protection Act 1998. Under this Act, an exemption from data protection requirements existed for companies who processed personal data for the prevention or detection of crime and the apprehension or prosecution of offenders.[19] This data could then be disclosed for these same purposes.[20] Under these provisions however, it was for the CSP to decide whether the law enforcement request complied with the stated exemptions; if they believed it did not, they could refuse to disclose the information. This meant that under these provisions, law enforcement may not be able to access the information which they believed was necessary to satisfy their investigative duties.

The Regulation of Investigatory Powers Act 2000 changed this policy by providing public authorities with the ability to access data in cases where disclosure is permitted by law. The authorities could access communications data which took the form of traffic data or subscriber data.[21] The data could be accessed for a range of purposes where the relevant investigator believed it was necessary to obtain communications data. Such

[19] Data Protection Act 1998 (DPA) s 29(1)(a) and 29(1)(b).
[20] DPA n(19) s 29(3).
[21] Regulation of Investigatory Powers Act 2000 (RIPA) s 21(4).

access could be granted, for example, in the interest of national security or for the purpose of preventing or detecting crime or of preventing disorder.[22] Access may also be granted in other instances, extending as far as for 'any purpose' which was deemed necessary by an order made by the Secretary of State.[23] Communications data under RIPA could therefore be accessed for a wide range of reasons; there was no requirement that the crime involved be serious. In making a request under RIPA, the investigator did not have to tightly define what information was sought; only that a broad category of communications data was required.[24] This allows, for example, for a request for all IP addresses that accessed a website, or all phone numbers that called a particular individual. The impact of this was that a large amount of data could be accessed; there was no requirement that collateral intrusion into this data be minimised.

This data must be sought for one of the specified purposes in RIPA s 22(2). However, these categories were interpreted broadly by those involved in granting access, principally, the designated person. The designated person was an established individual within a public authority who authorised applications made by investigators to access communications data. In law enforcement, this individual tended to be a superintendent or an inspector. As a general guideline, the designated person who authorised applications for communications data should have been separate from the investigation but this was not always practicable.[25] The designated person should have only granted an authorisation where he believed it was necessary and proportionate to the aim which was sought to be achieved.[26] While this legislation provided for a statutory underpinning for

[22]RIPA n(21) s 22(2).
[23] RIPA n(21) s 22(2)(h); The broad nature of these provisions meant that RIPA ended up being used for a wide range of purposes which weren't the aim of the legislation such as dog fouling, fly-tipping, and school catchment enforcement.
[24]RIPA n(21) s 23(2)(b).
[25] Anderson n(1).
[26]RIPA n(21) S 22(4).

the access of communications data by law enforcement, the provisions were very broad and made the data readily accessible. This raised concerns, particularly where access was being permitted to data in instances where it may be disproportionate to do so. For example, it was noted that 'in addition to the police investigating 'serious crime' and the security services and the police investigating terrorism, other agencies, such as local authorities, [could] access those data for relatively minor matters'.[27] The data was increasingly being subject to 'function creep' wherein it is used for purposes beyond national security or the investigation of crime.[28]

This was intensified by the significant number of authorities who could access the data under RIPA. The list of relevant public authorities allowed to access communications data under RIPA included bodies normally engaged in national security or law enforcement functions such as police forces, the National Crime Agency, Her Majesty's Revenue and Customs, and the intelligence services.[29] However, it also included any other public authority which was specified following an order made by the Home Secretary.[30] The ability of the Home Secretary to designate other authorities who could obtain this data was used expansively. As of 2015, there were approximately 600 organisations who could obtain communications data under the RIPA provisions.[31] The capabilities under RIPA exponentially increased the accessibility of the information.

It is worth noting that RIPA in its original iteration only applied to communications data collected for *ex post facto* investigations. This was because there was no consistent retention policy so it was unknown what data would actually be retained by the CSPs and

[27] HL Debates col 373, 20 March 2008.
[28] Clive Walker, 'Data retention in the UK: Pragmatic and proportionate, or a step too far?' (2009) 25 Computer Law & Security Review 325.
[29] RIPA n(21) s 25.
[30] RIPA n(21) s 25(g).
[31] Anderson n(1) 6.64.

therefore available for access. This limited the ability of law enforcement to find out information relevant to their investigations. The Crown Prosecution Service (CPS) and the police gave examples of how the inability to consistently access this data could hinder their investigations. They noted that 'conspirators become more guarded in their use of communications data as the moment of a crime approaches' and therefore older data may be more useful.[32] These interested parties argued that the data could tie relatively low level criminals to the higher ups in organisations by establishing patterns of communications using historic data. They also cited delays which occurred between incidents and the investigations which meant that older data often needed to be accessed.[33]

Increasing the accessibility of retained data mitigated this problem. The ability of law enforcement to access retained data did improve after the passage of the Code of Practice under Part 11 of ATCSA discussed in the preceding chapter. However, it is important to remember that Code only possessed a voluntary obligation to retain data. Therefore, the amount of data that could be accessed would be dependent on the decisions of the CSPs to retain the data. However, provided that information was retained, the Code could not place any restrictions on the ability of public authorities to access the data retained on condition that their authorisation for access satisfied the requirements set out in RIPA.

The provisions under RIPA were enacted to deal with the inability of public authorities to access information that they felt was relevant. The legislature guaranteed access in these provisions making the communications data under RIPA readily available to an increasing number of authorities and for a wide range of purposes. However, by expanding access to communications data, CSPs were faced with new obligations and the

[32] Anderson n(1) 9.45.
[33] Anderson n(1) 9.45.

risk of privacy intrusions intensified. CSPs had to facilitate access to the information required by the authorities, but were given no guidance or provisions on how to do so; nor were they entitled to challenge the requests made under RIPA. Increased data pools and lower accessibility thresholds meant that both more relevant data could potentially be accessed and more individuals could be caught by a request, thereby increasing the interference with privacy and the risk of collateral intrusions. These considerations informed critiques and judicial challenges to RIPA and drove subsequent legislative changes.

c. EU Law: Directives 2002/58/EC and 2006/24/EC

EU law in the field of data retention discussed in the previous chapter is largely silent on restrictions and provisions regarding access to the data by law enforcement. The principal provisions enshrined in these Directives concerned unauthorised access which interferes with the confidentiality of communications and related communications data.[34] However, the Directives did recognise that data retention was linked to later access by law enforcement. To that end, Directive 2002/58/EC required that providers establish procedures for responding to requests for access where those requests were issued by a competent national authority and in accordance with the legislative measures of the Member State.[35]

In amending Directive 2002/58, Directive 2006/24/EC similarly stressed the relationship between data retention and access and the importance of guaranteeing that the data be made available to law enforcement for a certain period but did not prescribe specific

[34] Directive 2002/58/EC states that measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications (Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (2002) OJ L201/37).
[35] Directive 2002/58/EC n(34) Art 15.

access conditions for the data.[36] Rather, decisions regarding access remained with the Member States. The Member States had to ensure that the data was provided only to competent national authorities in accordance with national law and set out procedures for accessing the data in accordance with the principles of necessity and proportionality.[37] There was no substantive or procedural guidance on the requirements that needed to be incorporated by Member States in so doing. Nor did the Directive effectively place any limitations on access and use of the data or require any safeguards to ensure against the potential interference with Article 8 rights. In mandating retention and providing for permissive access provisions these statutory instruments favoured the aims of law enforcement. However, they were open, and indeed were, challenged for the same procedures in the case of *Digital Rights Ireland.*

d. Joined Cases C-293/12 and C-549/12 Digital Rights Ireland v Minister for Communication & Ors and Seitlinger & Ors

As discussed in Chapter 3, the case of *Digital Rights Ireland* precipitated several legislative changes. The primary focus of the case was data retention systems provided for in the Directive. However, as noted, these systems are inextricably linked to access provisions; this was demonstrated by the applicant's argument that the obligation to retain data thereby *permitted control of and access to* the data in violation of fundamental rights. It is therefore instructive to examine the ruling of *DRI* as it relates to access.

In its holding, the Court affirmed that access by competent national authorities constituted a further interference with the right to private life under Article 8 ECHR and

[36]Directive 2006/24/EC of the European Parliament and the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications networks (2006) OJ L105/54 Recital 9.
[37] Directive 2006/24/EC n(36) Art 4.

Article 7 of the Charter.[38] Consequently, the interference can only be justified if it is done in accordance with law and in a manner which satisfies the requirements of necessity and proportionality. According to the Court, this required Member States to provide for domestic law which limited access and subsequent use of the data for the purposes of preventing and detecting precisely defined 'serious crimes' and enabling the prosecution of those crimes.[39] However, these 'serious crimes' were not defined in the Directive but in national law.[40] Indeed the Directive did not even impose a requirement that the data accessed was limited to the purposes of investigating and prosecuting 'serious crimes', only that access procedures, as established by the individual Member States, meet necessity and proportionality requirements.[41] As a result, the Directive failed to circumscribe when the data could be accessed.

Even though the Directive did require that data should only be accessed where necessary and proportionate, it did not lay down any objective criteria which would determine that the domestic access provisions met these requirements. There was no limitation on the number of persons entitled to access the data, meaning that it could be accessed beyond what was strictly necessary. Further, there was no requirement of prior review by a court or independent administrative body before access was authorised. Such procedures would guarantee that access to the data was limited and the use of that data was confined

[38] This confirmed the precedent set in: *Leander v Sweden* App no 9248/81 (ECtHR, 26 Mar 1987) para 48 which states 'Both the storing and release of such information…amounted to an interference with his right to respect for private life as guaranteed by Article 8(1)'; *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000) para 46: 'Both the storing by a public authority of information relating to an individual's private life and the use of it….amount to an interference.'; and *Weber & Saravia v Germany* App no 54394/00 (ECtHR, 29 June 2006) para 79: 'Furthermore, the Court,…, takes the view that the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference with the applicants' rights under Article 8'.
[39] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications & Ors and Michael Seitlinger & Ors* [2014] 2 All ER para 61.
[40] Directive 2006/24/EC n(36) Art 1(1).
[41] *DRI* n(39) para 61.

to what was strictly necessary for the criminal justice objective pursued.[42] While the primary result of the ruling in *DRI* was the invalidation of Directive 2006/24/EC, *DRI* also triggered changes in domestic legislation. National laws were subject to challenge if they did not provide the protections set forth by the Court.

e. Data Retention and Investigatory Powers Act 2016 and the Code of Practice for the Acquisition and Disclosure of Communications Data 2015

The UK recognised that *DRI* opened an avenue of potential challenge to the provisions regarding communications data. The Government therefore sought protect the capabilities of law enforcement clarifying the obligations placed on service providers under RIPA.[43] The clarifications under RIPA related primarily to rules regarding its extra-territorial effect wherein a CSP outside the jurisdiction of the UK could be obligated to obtain and divulge data to the UK upon issuance of a warrant.[44] However, the statutory changes in DRIPA did not relate to the domestic access provisions under RIPA. These changes were instead found in the amended Code of Practice for the Acquisition and Disclosure of Communications Data 2015 (hereafter the Code of Practice).[45]

In essence the *DRI* principles required that access be restricted to situations where it is necessary for the prevention, detection, or prosecution of 'serious crime'; where only a limited number of persons should be able to access and subsequently use the data for these purposes; and an independent administrative or judicial body is empowered to make decisions regarding access. The Code of Practice incorporated some of the

[42] *DRI* n(39) para 62. The safeguards and oversight regimes governing communications data are explored more fully in Chapter 6.
[43]Explanatory Notes to the Data Retention and Investigatory Powers Act 2014.
[44] Data Retention and Investigatory Powers Act 2014 s 4.
[45] This Code of Practice was issued pursuant to Regulation of Investigatory Powers Act 2000 s 71(4).

principles, but its overall ability to ensure access does not interfere with fundamental rights is questionable. In the first instance, the Code of Practice made no requirement that the powers of access only be used where it relates to 'serious crime'. Rather, the Code stated that the access will be considered necessary so long as the application provides how the requested information is linked to an event under investigation; how the person whose information they are seeking links to the event; what type of communications data is required; and what its link to the event is.[46] There was no requirement that the 'event' be a 'serious crime'. Further, the application would be considered proportionate if it justified the interference, taking into account any collateral intrusion and the ability of less intrusive means to gather the information, and stated how the information would benefit the investigation.[47] The provisions in the Code did not sufficiently limit access in the manner required by the *DRI* judgment.

Additionally, the large number of authorities who could access communications data remained. The one modification under DRIPA was the removal of the powers of access from thirteen authorities.[48] This does not reflect the principles in *DRI* that access to this data should be limited to where it is strictly necessary. Finally, under these instruments there was still no requirement of prior judicial authorisation or approval by an independent administrative body before access to the information was given. The authorisation was approved by a designated person. This individual was required to be independent from the operation and investigation for which the authorisation is given.[49] However, there were exceptions to this requirement of independence. For example, where it was necessary to act urgently, where there were small specialist units, or where

[46]Home Office, *Acquisition and Disclosure of Communications Data Code of Practice* (March 2015) para 2.37.
[47] *Ibid* paras 2.39 to 2.45.
[48] Regulation of Investigatory Powers (Communications Data) Amendment Order 2015 (SI 2015/228)
[49] Home Office, *Acquisition* n(46) para 3.11.

there were issues which required confidentiality, the requirements that the designated person be independent could be waived.

The provisions of the Code of Practice did not reflect the principles set forth in *DRI.* Nor did they provide significant protections from the interference which can result from these powers. Significantly, as a Code of Practice rather than a statutory instrument, there is little binding legal effect to its provisions. Indeed, s 74(2) RIPA notes that 'failure on the part of any person to comply with any provision of a code of practice…shall not of itself render him liable to any criminal or civil proceedings'. The Code was therefore an ineffective means of ensuring that data was acquired in a manner compliant with fundamental rights instruments.

f. Investigatory Powers Act 2016

As discussed in Chapter 3, the Investigatory Powers Act was passed to allow for the continued procedures of retention, while similarly updating the access powers for communications data in RIPA and giving statutory effect to some of the provisions set forth in the aforementioned Code of Practice.[50] Principally, the provisions under IPA deal with the issues which arose through the legal challenges. However, it is important to note the technological developments here as well. The increased production of data and limited categories which could be accessed according to legislation meant that law

[50] It is important to note that at the time of writing the Home Office, *Acquisition* n(46) remains the relevant code for these provisions. An amended Communications Data Code of Practice was issued in 2018 [Home Office, '*Communications Data DRAFT Code of Practice* (June 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/724394/CCS207_CCS0618947544-001_Home_Office_Publication_of_Codes_CLIENT_PRINTIN....pdf> accessed 7 July 2018]. It is envisaged that this Code will come into effect following the passage of The Data Retention and Acquisition Regulations 2018 [Draft SI 2018 No Electronic Communications The Data Retention and Acquisition Regulations 2018 <http://www.legislation.gov.uk/ukdsi/2018/9780111170809/regulation/4> accessed 12 July 2018]. These Regulations have been laid before Parliament (as of 11th July 2018) but have not yet been made as a UK Statutory Instrument. Where necessary, the provisions of the Draft Code, as they relate to the access procedures discussed in this chapter, will be noted in the footnote until such a time as they come in to force.

enforcement '[had] access to a decreasing proportion of an increasing quantity of digital information' under the old law.[51] IPA therefore seeks to ensure that the access provisions remain, without imposing any undue limitations on law enforcement's capabilities in this area, while simultaneously increasing the categories of information that can be collected.

For example, the IPA retains the authorisation procedures of its predecessors. Mainly, authorisation can still be granted by a designated senior official, where it is deemed necessary and proportionate.[52] In adjudging proportionality and any threat of collateral intrusion that might arise from access, the considerations are based on the time the application is made, and prior to any interference.[53] This imposes an element of temporality in the process and is significant to the context in which privacy interest might be triggered. Whilst when an application is made these measures may satisfy the proportionality requirements, the act of the interference and the subsequent investigation may reveal that the access was indeed disproportionate and unnecessary. This issue is exacerbated by the increasing tendency to access communications data as a preliminary route of investigation rather than one which only occurs once other investigative methods have been exhausted. Whilst it is not possible to foretell all potential implications for privacy, these factors should be considered in making an application.

In approving the application, the designated official cannot be involved in the investigation but this requirement can be waived in exceptional circumstances.[54] The application must provide information relating to why and by whom the information is sought.[55] Furthermore, additional reporting and recording requirements are imposed on

[51] Clive Norris and Gary Armstrong, *The Maximum Surveillance Society* (1999 Berg) 209.
[52] Investigatory Powers Act 2016 s 61(1).
[53] Stanley Burnton, *Report of the Interception of Communications Commissioner* (2016, HC 297) 7.46.
[54] IPA n(52) s 63.
[55] IPA n(52) s 64.

the authorities who make access requests.[56] The list of authorities who can access the data remains expansive but additional obligations are now required if local authorities require access.[57] In practice, law enforcement agencies account for approximately 94% of access requests and investigating crime is the primary justification for access.[58] However, there remains no requirement that the data only be accessed for the investigation of 'serious crime'. Once a request is approved by the designated person, it is communicated to a Single Point of Contact (SPoC) who is trained to facilitate the lawful acquisition of communications data and effective cooperation between public authorities and CSPs. The SPoC performs an oversight role by advising applicants on the interpretation of the law and ensures that the application is free from errors and lawful.[59] These provisions ensure the access capabilities of law enforcement are preserved in the new legislation.

Whilst the access provisions have remained relatively static since 2000, the Act does take into consideration technological developments which have increased the amount of data available and attempts to ensure that this data is made accessible as well. As discussed in Chapter 3, the IPA allows for the retention and then subsequent access of internet connection records (ICRs) which 'are a record of the internet services that a specific device connects to – such as a website or instant messaging application – captured by the company providing access to the internet'.[60] The IPA provides that public authorities can access this data to identify: the sender of a communication, which communications

[56] Home Office, *Acquisition* n(46) 6.1 sets the record keeping obligations concerning applications and their outcomes; urgent authorisation; and relevant information about the type of data to whom it relates. CSPs must similarly retain records of the access requests received and the information they provided to comply (6.3).
[57] IPA n(52) s 70
[58]Burnton n(53). 85.8% of access request relate to preventing or detecting crime or preventing disorder. The largest proportion of crime types are drug offences at 24%; sexual offences 12%; theft 9%; and fraud and deception at 8%.
[59] Burnton n(53).
[60]Explanatory Notes to the Investigatory Powers Act 2016 s 87 para 265.

services a person has been using (i.e. apps on their phone), where the person accessed illegal content, or which internet service is being used and when and how often.[61] The authorisation which grants access to the information for these purposes must be deemed necessary by the designated official.[62] The authorisation can also be granted where it is necessary for the prevention or detection of crime where that crime is serious or classed as 'other relevant crime'.[63] It is not readily apparent why the Act distinguishes between preventing and detecting relevant crime and preventing or detecting 'serious crime' as the provisions concerning the two are the same. Regardless, this new category of data potentially increases the investigative capabilities of law enforcement.

However, the incorporation of this technological development into law enforcement procedures raises issues with the social norms typically ascribed to this sort of information. ICRs have the ability to reveal a significant amount of information about an individual as they give a picture of, for example, the websites an individual visits on a particular day. In order to minimise the intrusion by preventing the disclosure of content, the law limits the ability of the requesting authority to look beyond the first backslash in these records; so, for example, www.google.co.uk would be accessible but with www.google.co.uk\investigatorypowersact, the investigatory powers act would be omitted from the record as it is deemed content.[64] This is relatively innocuous when examining basic websites like Google or Facebook but becomes much more personal

[61] IPA n(52) s 62(3) & 62(4).
[62] IPA n(52) s 61(7) sets out when it will be necessary to obtain this data, such as in the interest of national security or for the purpose of preventing or detecting crime or of preventing disorder.
[63]IPA n(52) s 62(5); other relevant crime here is crime which is not serious but where the offence, or one of the offences, which would be constituted by the conduct concerned is an offence for which the individual is capable of being sentenced to imprisonment for 12 months or more, or an offence by a person who is not an individual or which involves, as an integral part of it, the sending of a communication or a breach of a person's privacy. (IPA n(52) s 62(6)).
[64] This distinction to prevent content of the website being disclosed does not function particularly well with the technology. For example, bbc.co.uk/news would omit 'news' as content but news.bbc.co.uk, which takes you to the exact same site, would not be deemed content because it comes before the first backslash.

when it potentially concerns sites that have more descriptive domain names. As a result, intrusive personal information can be garnered from ICRs. This information can both identify potential targets for law enforcement and more broadly identify sites which 'might be suggestive or corroborative of criminality'.[65] This is one of the reasons it is so valuable to law enforcement. In permitting the retention and access to ICRs, the IPA extends the traditional powers of law enforcement to intrude into areas where it was not feasible before; this development has been facilitated by technology, but it also fails to take into consideration the wider social impact which results from treating this new and more intrusive category of data in the same manner as traditional communications data.

The IPA seeks to go even further in providing access to law enforcement by requiring CSPs to create and install technical capabilities which provide for quicker access and process the data so that only relevant information is disclosed to the public authority, thereby removing the risk of collateral intrusions. Previous provisions regarding the creation of such technical capabilities were undertaken under the powers of RIPA but only as regards interception. The Investigatory Powers (Technical Capability) Regulations 2018 extend these powers to communications data as well. The regulations aim to ensure that law enforcement can obtain communications data without undue delay, and requires CSPs to create, modify, test, and maintain systems which enable them to do so.[66] CSPs are further required to only disclose, where practicable, the communications data which is authorised; no extraneous data should be disclosed.[67]

[65] Anderson n(1) 9.59.
[66] Investigatory Powers (Technical Capability) Regulations 2018, SI 2018/353 Schedule 2.
[67] IP Regulations n(66) Schedule 2 Part 1(8); It is worth noting that this raises a question as to whether it would absolve the public authority of any liability for a privacy violation resulting from a collateral intrusion of the data if the obligation was placed on the CSP to filter this out. If so, is there any right to remedy which can be sought against a CSP who mistakenly discloses additional irrelevant information? This will be addressed in Chapter 6.

Further, CSPs are required to provide the information sought in an intelligible form and remove any electronic protections which have been applied to it.[68] Essentially this provision requires that, where possible, encryption be removed from the data so that law enforcement can utilise it for criminal justice purposes. However, depending on the encryption methods, it may not be possible to remove this protection to provide the police access to the desired information.[69] Sir Thomas Winsor, HM Chief Inspector of Constabulary in his State of Policing Report claimed that, 'The wide availability of impenetrable end-to-end encryption services has made life easier for terrorists, paedophiles, and organised criminals, and harder for law enforcement'.[70] The provisions of the Regulations in this regard demonstrate how the needs of law enforcement have been incorporated into this secondary instrument as a result of technological developments which made encryption more accessible to everyday users and therefore the data more difficult to acquire and interpret.

In addition, the Regulations make provision for the Secretary of State to require CSPs to install and maintain any apparatus provided by or on behalf of the Secretary so the operator can obtain or disclose communications data.[71] This is billed as a communications data acquisition 'black box' which is designed and implemented by the Government rather than by private companies. There is very little information provided about what these apparatuses might do, only that if so required the CSP will be required

[68] IP Regulations n(66) Schedule 2 Part 1(9)
[69] This is the case with messages sent over WhatsApp, an over-the-top messaging service, which offers users end-to-end encryption for their communications. This type of encryption means that it is not possible for law enforcement to access the content of those communications. However, WhatsApp does not encrypt the metadata (akin to communications data), so LEA capabilities would not be hindered in this area. Thomas Fox-Brewster, 'Forget About Backdoors, This is the Data WhatsApp actually Hands to Cops' (*Forbes* 22 June 2017) <https://www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/#64dda5141030> accessed 27 July 2018.
[70] HMCIC, *State of Policing: The Annual Assessment of Policing in England and Wales* (2017) <https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/state-of-policing-2017-2.pdf> accessed 8 May 2018.
[71] IP Regulations n(66) Schedule 2 para 10.

to place them in their system. Finally, there is an obligation placed on service providers to inform the Home Office prior to any changes to their services or instituting any new technologies which may impact on these capabilities.[72] CSPs may also be required to consider the requirements of the technical capability regulations in designing their products and services. The effect of these regulations requires CSPs to perform further functions of a public nature by creating infrastructure which provides access and disclosure. As a result, the provisions of the IPA regarding access intrude significantly farther than its forebears into the personal information of individuals.

g. Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson & Ors

The final element to be considered in the discussion of access to retained data in the ICT systems is the *Tele2* case. As regards access, the applicants in *Tele2* sought to determine whether: 1) access by national authorities can be permitted for the data retained under the general obligation imposed by Article 15(1) Directive 2002/58;[73] and 2) whether the *DRI* judgment lays down any mandatory requirements applicable to Member States' domestic law for access in order to comply with Articles 7 and 8 of the Charter.[74] In answering these questions, the Court had to first consider whether access fell within the scope of Directive 2002/58. In this regard, Member States' laws interpret the scope of the Directive differently; notably, for the purposes here, the UK argues that it is only legislation relating to retention, but not access, which falls within the scope of the Directive.[75] This viewpoint was supported by the Commission. However, the Court

[72] IP Regulations n(66) Schedule 2 para 11.
[73]Joined Cases C-203/15 *Tele2 v Post-och telestyrelsen & C-698/15 Watson & Ors v Secretary of State for the Home Department* (2016) ECLI 970 para 51.
[74] *Tele2* n(73) para 59
[75] *Tele2* n(73) para 65. There is disagreement amongst the domestic law of several Member States as to whether national access legislation falls within the scope of the Directive. Belgium, the Netherlands,

found that the scope of the Directive went farther and incorporated the legislative measures relating to access to the data retained as well:

> Further, since data is retained only for the purpose, when necessary, of making that data accessible to the competent national authorities, national legislation that imposes the retention of data necessarily entails, in principle, the existence of provisions relating to access by the competent national authorities to the data retained.[76]

As access was held to fall under the Directive, the question then became to what extent there existed any requirements in national law to ensure that access provisions complied with relevant fundamental rights standards, and relatedly, whether the requirements of independent oversight and purpose limitation set out in *DRI* were mandatory. In determining the question, the Court noted that the access provisions must satisfy the requirements of necessity and proportionality. Therefore access must only occur where strictly necessary and be subject to adequate safeguards which clearly prescribe when access will be authorised. Further, access must only be granted where necessary for those purposes relating to 'serious crime';[77] namely where that access relates 'to the data of individuals suspected of planning, committing, or having committed a 'serious crime', or of being implicated in one way or another in such a crime'.[78] However, the precedent set here runs counter to the policies set out in the IPA wherein increasing categories of data can be accessed without being linked to any 'serious crime'.

Denmark, Germany, Estonia, and Ireland believe that it does. The Czech Republic believes that it does not.

[76] *Tele2* n(73) para 79.
[77] *Tele2* n(73) para 115.
[78] *Tele2* n(73) para 118.

The ruling serves to limit the amount of data that can be accessed and thereby the powers of law enforcement in this regard. This is significant as the police have expressed views that communications data is valuable for even minor investigations. In his report, David Anderson noted that 'Communications data may also be needed in order to meet public expectations that the police will be able to solve even relatively low-level crimes. Thus, where someone has their mountain bike stolen and sees it advertised for sale…, investigators may need to apply, at a minimum, for subscriber information to pursue the case'.[79] In limiting access, these lower level functions will not be permitted. Proponents argue that this will hinder the overall abilities of law enforcement, however, such provisions serve to offer protections for individuals by reducing the potential collateral intrusions and guaranteeing that the data accessed is confined to that which is necessary.

Domestically, the Court of Appeal case to apply the ruling in *Tele2 and Watson* agreed with the requirement that Section 1 DRIPA was inconsistent with EU law in that it failed to limit access to retained data solely for fighting 'serious crime'.[80] Further, access was not made contingent on prior review by a court or an independent administrative authority.[81] As a result, the Court of Appeal granted declaratory relief in this case. The issue of access was subsequently raised in the High Court case of *Liberty v SSHD* wherein the access provisions under the IPA were challenged. In this case, the claim for judicial review succeeded as retention under IPA was held to be incompatible with fundamental rights due to the fact that subsequent access was not limited to 'serious crime' nor was it subject to prior judicial or independent administrative review.[82] In

[79] Anderson n(1) 9.26.
[80] *Watson v SSHD* [2018] EWCA Civ 70 para 13.
[81] *Watson* n(80) para 27.
[82] *Liberty v SSHD* [2018] EWHC 976 para 186.

consequence, the Court held that the legislation must be amended by the 1 November 2018 to address the current inadequacies of the access regime.

IV. Applying Contextual Integrity to Access

In determining whether privacy has been violated as a result of access to communications data, it is necessary to determine the extent the informational norms have shifted, thereby breaching contextual integrity. To this end, it is necessary to examine whether the norms associated with information types, transmission principles, and actors have been altered by the developments of the system. In the context of the ICT system at issue, the attributes of communications data mean that far more information can be derived from it. This makes the ability to access that data a valuable tool for law enforcement. Legislative developments in this area reflect the desire to increase access and ensure that the information is available for the necessary purposes. Concurrently, the increase in data poses an additional risk to the individual. The information which can be accessed does not only concern basic data on communications (i.e. who called whom and when), but encompasses far more personal details, such as what websites an individual visits. The intrusiveness of this information would be recognised if it occurred in a different context.[83] However, because these interferences occur in the digital realm, their intrusiveness is not recognised as such.

To assess whether the informational norms associated with access to communications data are breached, it is first necessary to construct these norms by looking at the information types, transmission principles, and actors involved. With regards to the

[83] Consider for example targeted surveillance wherein an individual was followed to every location they visited throughout the day, who they spoke to in each location was noted, and the time they spent there was recorded. Such an action would be subject to strict safeguards and oversight provisions which do not exist in the case of communications data.

information type, the question is whether the nature of the information has changed in some way which would alter the norms attributed to it. In the legislative discourse, communications data is frequently likened to envelope information; this type of information exposes the identities of a person's colleagues and friends revealing associational ties. Even this type of information raises concerns for privacy as in many instances, people may care more about concealing with whom they are talking than what they are saying. However, beyond the mere nature of the data which can raise privacy issues, there is the issue of the technology which collects, maintains, and provides access to it. The data is centralised, digitised, and structured; it is not mediated by human memory or relationships.[84] Whereas in past, the information would be sought from human actors, the digitised information is stripped of its context and surrounding factors. It is a representation of fact but not necessarily meaning. Furthermore, the information which law enforcement seeks to access is not constrained by previous temporal considerations; the data is not only forward looking but historic data as well. It is access to multiple communications sources, reaching back in to the past, which can be used to track and monitor individuals. Nor does the nature of the information neatly fit into the confines of the definition of 'envelope data'. This data is expansive and, particularly with the inclusion of ICRs, reveals intimate and highly personal details. Whilst the access provisions differ between content and communications data, in practice this distinction has become difficult to make.

In addition to changes relating to the nature of the information, the development of the ICT system has altered norms associated with the transmission of information. Notably for the access component, constraints on the flow of information have changed as a result

[84] Lisa Austin, 'Technological Tattletales and Constitutional Black Holes: Communications Intermediaries and Constitutional Constraints' (2016) 17 Theoretical Inq L 451, 457.

of legislative developments. Jurisprudence concerning data has confirmed that communication of that data to a third party, including a public authority, constitutes an interference with the right to respect for private life, regardless of the subsequent use of the information.[85] By granting access from these third parties to public authorities the norms associated with information flows have changed. Furthermore, access is increasingly granted regardless of the traditional jurisdictional bounds which applied prior to the development of technology which enables the sharing and spread of data transnationally. There is often a disconnect between the location of the entity seeking access and the intermediary who possesses the information. The Government argues that it is the location of access, not the location of data, which is relevant to jurisdictional concerns,[86] and this is reflected in the legislation. Yet, the disconnect between access and data strips the data of any residual links to a community or society that might exist. As such, the meaning of the data becomes removed from the events from which it was derived. Changes to the traditional flow of information associated with communications data are compounded by shifts in the roles played by the relevant actors in the system.

Several actors are involved in the access processes of the ICT system and the roles they play also play a role in altering entrenched informational norms. It is necessary to determine who is in charge of access as the attitudes, predispositions, and biases of those actors can fundamentally shape the process.[87] The subjectivities of those who direct the choice of information accessed will be relevant to the value ascribed to that data. As has

[85] CJEU, Opinion 1/15 on the Draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, Opinion of the Court (Grand Chamber), 26 July 2017, paras. 124-125.
[86] Jennifer Daskal, 'The Un-Territoriality of Data' (2015-2016) 125 Yale L J 326, 373; IPA s 85 states that an authorisation may relate to conduct or persons outside the UK.
[87] Kevin Haggerty, 'Tear down the walls: on demolishing the Panopticon' in Lyon (ed), *Theorizing Surveillance: The Panopticon and Beyond* (Willan Publishing 2006) 33.

been noted in the legislation, certain public bodies have purpose limitations which apply to their access requests or the type of data they can access.[88]

The CSP acts principally as a facilitator for access, providing the basic necessary infrastructure to be able to disclose the required information to investigators. In this regard, the CSP acts as a conduit; information is collected and retained on their system and, in the same manner and form, it is passed on to investigators. The delegation of this power to private entities has a considerable impact on norms associated with access. Notably, there exist immunities for companies who comply with legitimate access requests. 'As a result, these companies are subject to neither the burden of transparency nor the constitutional constraints imposed upon state actors'.[89] Information which is incorrect or shared erroneously by the CSP will not give rise to liability under the Investigatory Powers Act.[90] The requirement that CSPs act as facilitators here can enable the subversion of traditional protections concerning access. Typically, a public body will be limited in the manner in which it can search through electronic information. By requiring CSPs to do this, traditional limitations and protections for fundamental rights are more easily avoided.[91]

[88] For example, the power of officials in the Criminal Cases Review commission may only make requests relating to miscarriages of justice. The Scottish Ambulance Board is limited to requests with the aim of preventing or mitigating injury or death. JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age* (2011) < https://2bquk8cdew6192tsu41lay8t-wpengine.netdna-ssl.com/wp-content/uploads/2015/01/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf> accessed 25 Nov 2015 74.

[89] Nancy Kim and Jeremy Telman, 'Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent' (2015) 80 Mo L R 723, 745; Take an example from the United States. There the Foreign Intelligence Surveillance Act offers immunity from breach of contract claims when they share information with the government in violation of privacy provisions in their agreements with customers [Federal Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub L No 110-261, ss 702(h)(3), 703(e), 122 Stat 2436 (2008)]

[90] This is the case under the Investigatory Powers Act 2016 Part 3. However, companies may still be held liable for data breaches under the Data Protection Act 2018.

[91] Niva Elkin-Koren & Eldar Haber, 'Governance by Proxy: Cyber Challenges to Civil Liberties' (2016) 82 Brooklyn L R 105, 107.

Additionally, more technical requirements are now being placed on CSPs to not only provide access, but to process the data in a manner that limits collateral intrusions and limits any delays for law enforcement in acquiring the information. As Leenes and Koop recognised, the legislation has directed the technology providers to build in features related to legal norms, and industry has complied.[92] The additional requirements placed on CSPs to process and interpret the data demonstrates a shift in the role assigned to this organisational element. They are more actively involved in the criminal justice processes and the legislative developments indicate that this is an area where the requirements placed on them are likely to expand further in the future. This is a fundamental shift which has altered the informational norms, as access is no longer solely in the purview of law enforcement, but has been expanded to CSPs as well.

Concurrently with the increased role of CSPs in the process there has been a diminution of the role of the individual and an increase in the informational disparity between parties. Individuals are prevented from having knowledge of access and how their information is used. Companies, in deciding whether to comply or challenge an access request, can exercise their discretion in a manner that best comports with their own corporate interest, rather than any interest for the individual. Austin argues that this sort of cooperation 'is free of the kinds of personal interest or prejudice that raises questions with other [parties]. However, it also seems to be free of other kinds of constraining social norms such as the loyalty characteristic of various social relations'.[93] As a result, changes in the roles played by the actors involved in the access process, along with alterations in the nature of information and its flow reflect shifts in informational norms.

[92]Bert Jaap Koops & Ronald Leenes, "Code" and the Slow Erosion of Privacy' (2005) 12(1) Mich Telecom & Tech L R 335.
[93] Austin n(84) 456.

Such shifts are indicative that contextual integrity has been breached in the context of the access element of the ICT system.

V. Conclusion

For law enforcement, the access component of the ICT system has evolved to allow for the acquisition of more data. The overall objective, of accessing communications data for the investigation of crime, has been preserved by legislative developments. The organisational element, in the form of CSPs, has seen its role gradually increase as they take on more duties which facilitate the criminal justice processes. Individuals have also seen a shift in their position, as the communications data they generate provides more information which can be accessed. Technological developments have increased the generation of this data and enabled the creation of processes and methods whereby the CSPs can provide simpler and quicker access to law enforcement. As a result, the informational norms associated with access to communications data have been altered. The changes to the access component have failed to incorporate these changes in norms and therefore there is a *prima facie* breach of privacy when communications data is accessed. While access can be classed as a violation of privacy, it is also important to examine what is done with the accessed data. How, and for what purposes is it analysed? The following chapter looks to the analysis of accessed communications data in the ICT system, and how that might result in privacy violations.

CHAPTER 5: ANALYSIS OF COMMUNICATIONS DATA

I. Introduction

In the ICT system, communications data, retained and accessed, requires analysis to determine the value of the information and how it can be best applied to meet criminal justice aims. It is therefore necessary to establish what processes and methods are used to extract meaning from the information. Technological growth is a key element in the development of these methods. Analytical processes have improved significantly due to technological advancements in areas such as information science, information management, mathematical and statistical analysis, cryptography, and artificial intelligence.[1] As demonstrated in the previous chapters, laws have similarly developed, requiring new methods of data capture, processing, and access, thereby providing more information to be examined. The utility of communications data for investigations has motivated the development of increasingly sophisticated methods for interpreting the collected information.

Similarly, the ability to analyse and use this information in an effective manner has, to an extent, altered the nature of policing, allowing investigators to eschew traditional techniques and take a more proactive approach. Communications data can be used as a preliminary investigative tool which is then used to gather more persuasive evidence, as well as being a source of information to strengthen a case against an identified suspect. Provided meaningful information can be extracted from the communications data, the data then allows police to build applications for more intrusive investigative methods or

[1] Helen Nissenbaum, *Privacy in Context* (Stanford University Press 2010) 37.

renders those measures unnecessary.[2] The value of the data reaches into other areas of the criminal justice process as well. For example, prosecutors can use the analysed information to demonstrate patterns of communications between conspirators.[3]

The role of the data in the criminal justice system motivates the continuing development of processes which enhance analytical capabilities. There are several broad categories of methods of analysis which are of significance for communications data and law enforcement. Algorithmic processing, aggregation, and Big Data analysis are three of the principal ways in which meaning can be derived from the data. The technology is used to create or extract information which goes beyond what can be found naturally or what is voluntarily reported.[4]

The first category broadly refers to the use of computer algorithms to draw inferences from data. This applies to communications data when it is used to infer suspicion or guilt based on the movements or contacts an individual has made. It is particularly useful when attempting to discover information about a wider criminal network from the information provided by a relatively low level criminal. As Ian Brown notes, 'most people's communications behaviour patterns are extremely regular, and investigating a small number of carefully chosen individuals based on these patterns can reveal information about much larger networks'.[5] The use of algorithms which engage with automated processes, such as the 'request filter' which will be discussed in this chapter, raises significant concerns for human rights.

[2] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (Stationary Office 2015) 9.30.
[3] Anderson n(2) 9.32; this is particularly useful in organised crime cases.
[4] Gary Marx, 'Surveillance Studies' in Wright (ed) *International Encyclopaedia of the Social & Behavioural Sciences* (2 edn, Elsevier 2015) 735.
[5] Ian Brown, 'Communications Data Retention in an Evolving Internet' (2010) 19(2) International Journal of Law and Information Technology, 101.

In addition, aggregation as an analytical process brings together various strands of information to allow determinations to be made. The extensive nature of the data and technological developments which enable digital processing and analysis are much more powerful than previous capabilities which relied on human capacities. More meaning can be extracted from the information using these digital processes as well. As Nissenbaum notes, 'Abetted by brute processing power, increasingly sophisticated mathematical and statistical techniques have made it possible to extract descriptive and predictive meanings from information that goes well beyond its literal boundaries'. [6] In order to achieve this, the information that is aggregated needs to be rendered into recognisable data, with CSPs generating and retaining the data in a consistent manner. Even within setting the requirements for the consistent collection and processing of data, there are inscribed politics and social constructs which must be acknowledged.[7]

Finally, and related to the two preceding methods, Big Data techniques allow for the creation of large scale data sets. These data sets can aggregate data in the manner listed above, or offer pools of information to be analysed using algorithmic processing. They also facilitate the creation and maintenance of databases which enable the sharing of information and the detection of patterns and correlations. This allows individuals to be identified and their current actions linked to their biographical profile.[8] This capability is important, as without bulk machine based techniques, it is much more difficult for investigators to link crimes to a person, discover the identity of individuals using a communications service, identify relevant locations, or separate communications data and content from one another.[9] Such methods further enable pre-emptive policing

[6] Nissenbaum n(1) 42.
[7] Tarleton Gillespie, 'The Relevance of Algorithms' in Gillespie Boczkowski and Foot (eds) *Media Technologies: Essays on Communication, Materiality, and Society* (MIT Press 2014) 167, 171.
[8]Clive Norris and Gary Armstrong, *The Maximum Surveillance Society*, (Berg 1999) 219.
[9] Anderson n(2) 9.34.

techniques in which large scale data sets are used to cluster data in such a way that information is inferred and predictions can be made.[10]

The analytical techniques at issue in the ICT system possess the three preceding capabilities. However, the analysis of the data goes beyond these three areas. Whilst the analytical processes referred to above highlight how CSPs have been further co-opted into the law enforcement process through the additional functions imposed on them, it is also important to examine the analytical techniques of law enforcement themselves. To that end, it is necessary to examine law enforcement use of, and subsequent downstream access provided to, data. These processes must be judged against their impact on context relative informational norms and determine whether there has been a shift in these norms which represents a disproportionate interference with privacy. This chapter proceeds by examining four methods of analysis which are embodied in the communications data provisions of the investigatory powers instruments: Part I will examine IP address resolution, Part II will address the interpretation of Internet Connection Records (ICRs), and Part III will analyse the 'request filter'. Each of these methods is a result of technological advances which both motivated the development of a legal framework to provide law enforcement access and fundamentally shifted the social norms ascribed to the analysis of data. Each element will be examined in turn. Part IV will address the subsequent sharing and downstream use of this data to satisfy law enforcement functions. Such sharing occurs once the data has been analysed for its initial purpose and provides an additional information source for law enforcement. Part V will then proceed by assessing the impact of these technological developments on the context relative

[10] Rosamunde Van Brakel and Paul De Hert, 'Policing, surveillance and law in a pre-crime society: Understanding the consequence of technology based strategies' (2011) 20 J of Police Studies 163, 173.

informational norms typically associated with the analysis of communications data to establish that there has been a breach of contextual integrity.

II. The utility of communications data analysis in IP Address Resolution

IP address resolution refers to the linking of IP addresses to a physical location. Proponents of IP address resolution erroneously cite its ability to enable law enforcement to link an individual to an IP address at a given time.[11] Such a belief has motivated the inclusion of the retention of IP address information in the relevant legislation.

a. Legislative Provisions Concerning IP Addresses

As discussed in Chapter 3, the Data Retention Regulations 2009 were the first instrument to mandate the retention of internet access, internet e-mail and internet telephony communications data. Under these regulations, CSPs were required to retain data necessary to trace and identify the source of a communication and the date, time, and duration of a communication.[12] IP addresses fell under this category. However, the retention of relevant information concerning IP addresses did not enable the law enforcement to link this data to individuals. Additional information was needed to achieve this, leading to the legislative developments in the subsequent Counter Terrorism and Security Act.

In order to facilitate the ability to link IP addresses to individuals, the CTSA extended the categories of information that needed to be retained to include any data that was necessary to achieve this goal. The Explanatory Notes for the CTSA discussed the

[11] Ramakrishna Padmanabhan Amogh Dhamdhere, et al, 'Reasons Dynamic Addresses Change' (ACM-IMC, Santa Monica, November 2016) 183.
[12] The Privacy and Electronic Communications (EC Directive) Regulations 2003 SI 2003/2426 Schedule 1 Part 3 ss 11 and 13.

necessity of this provision, 'An IP address is automatically allocated by a network provider to a customer's internet connection, so that communications can be routed backwards and forwards to the customer. [CSPs] may share IP addresses between multiple users. The providers generally have no business purpose for keeping a log of who used each address at a specific point in time'.[13] As a result, in the absence of specific statutory provisions, information which was of use to law enforcement in their investigations was being deleted. The CTSA mandated retention of data that can be used to identify which IP address belonged to which individual.[14] However, no specific additional categories of data which might assist in this were explicitly set forth in the legislation. As such, it is questionable whether or not CSPs are under an obligation to retain this additional information as it lacks a statutory basis. Without the retention of additional information, IP addresses possess little value for law enforcement, as will be shown below.

b. Effective IP Address Resolution: Processes and Problems

In order for IP addresses to be of use to law enforcement, the investigating bodies need to be able to link an individual or an account to the IP address involved in the potential illicit activity. However, the current nature of IP addresses frustrates this aim. Under the current system, also known as IPv4,[15] there are a finite number of IP addresses. As such,

[13]Explanatory Notes to the Counter-Terrorism and Security Bill 2014 para 121.
[14] Notably, the legislation permits the retention of 'other identifiers' to enable IP address resolution. The explanatory notes to the Act note that this could include port number or MAC (media access control) addresses. Explanatory Notes to the Counter-Terrorism and Security Act 2015 para 96.
[15] It is worth noting that the new version of IP addresses known as IPv6 provides an unlimited number of IP addresses and would therefore not be subject to this problem. However, the switchover from IPv4 to IPv6 is time and cost intensive and is not yet in place in the UK. [OFCOM, *Report on the Implications of Carrier Grade Network Address Translators* (2013 MC/159) 7]. This can be contrasted with the case of Belgium which leads the world in the rate of IPv6 adoption [Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (Communication) 2017 JOIN 0450 final 14.] As the UK has not adopted IPv6 to any significant degree, the analysis here focuses on the issues with IPv4 which are most relevant to this analysis.

CSPs have adopted technical means to share the limited number of IP addresses between their users. This process is known as Carrier Grade Network Address Translation (CGN).[16] Essentially this technology enables IP addresses to be shared between multiple subscribers at the same time. The sharing of IP addresses through this technology has serious implications for the ability of law enforcement to use the information. As Rob Wainwright, Director of Europol noted when discussing the implication of CGN for policing: 'It might mean that individuals cannot be distinguished by their IP address anymore, which may lead to innocent individuals being wrongly investigated by law enforcement because they are sharing their IP address with several thousand others – potentially including criminals'.[17]

The use of CGN technology has direct implications for privacy. As IP addresses are shared between many users, any request to access this information will disclose the data of a large pool of individuals.[18] Such a process makes it difficult to limit collateral intrusions or interferences with the privacy. Any subsequent analysis which involves processing this large data set to refine it further represents a privacy interference. Due to this technology, requests for IP addresses actually require law enforcement to investigate many more people than would normally be necessary. In requesting the information, law enforcement will have to be very precise if this collateral intrusion is to be limited. For example, the investigators must specify both the IP address and the time at which they

[16] CSPs are increasingly adopting this technology, with 90% of industry using it for mobile internet and 50% for fixed line. Europol, 'Are you sharing the same IP address as a criminal? Law enforcement call for the end of carrier grade nat (CGN) to increase accountability online' (Europol Press Office) < https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online> accessed 18 Oct 2017.

[17] *Ibid*

[18] Furthermore, it has been held that IP addresses constitute personal data where an individual can be identified from that information, even where a third party, including a public authority, must obtain additional data for the identification to occur. See: *Patrick Breyer v Bundesrepublik Deutschland* (C-582/14) [2016] ECLI 770 para 49; Court of Cassation (Cour de Cassation), Arrêt No. 1184 du 3 novembre 2016, 15-22.595, 3 November 2016 [France].

believed the relevant communication occurred. The timing must be accurate; 'if there are timing mismatches then a different subscriber could be using the IPv4 address than the one who needs to be traced'.[19] However, the ability to identify a time is frustrated by technical issues. Frequently, servers where the relevant information is stored are not synchronised with their timestamps. This means that the IP address captured at a specific data and time by, for example Facebook, may vary from the time used by Vodafone in the UK whose service accesses the site.[20] This will result in the search parameters being widened and more results being returned which raises further concerns for privacy.

There are implications for the companies required to retain the addresses as well. If IP addresses are shared, there is no unique identifying information. As Mackey et al note, 'using an IP address to identify a specific individual is problematic because there is nothing about the addresses themselves that make them personally identifiable. IP addresses identify particular devices or groups of devices on the Internet, not people using the Internet'.[21] In order for a CSP to identify an account associated with an IP address, they would need to retain further information, such as a port number. Such requirements make the technical analysis more involved. As was noted in the OFCOM report concerning CGN,

> The only party with the relevant knowledge or control in a CGN scenario will be the ISP and this will likely increase the frequency and complexity of requests from

[19] OFCOM n(15) 54.
[20] Joint Committee, Written Evidence for the Investigatory Powers Bill Law Enforcement Submission 5.
[21] Aaron Mackey Seth Schoen and Cindy Cohn, 'Unreliable Informants: IP Addresses, Digital Tips, and Police Raids: How Police and Courts are Misusing Unreliable IP address Information and What they can do' (EFF 2016) 6.

law enforcement or third parties, diving up costs for ISPs and potentially exposing them to legal liability arising from such decisions.[22]

Even where the IP address resolution is not frustrated by processes such as CGN, errors are highly likely to occur. Indeed, in his final report as Interception of Communications Commissioner, Sir Stanley Burnton noted that the most serious errors with acquiring communications data occurred with IP addresses. Most of the errors are transcription errors which can occur when IP address numbers are transposed, the wrong date/time format is used, the wrong time zone is used, or the relevant address is misheard or misstated during an urgent oral application. These errors can have potentially devastating impacts. Burnton described the impact of these errors, 'People have been arrested for crimes relating to child sexual exploitation. Their children have been taken into care, and they have had to tell their employers'.[23] Further errors have resulted in individuals being wrongfully arrested and their home and devices searched.[24] The potentially devastating impact of errors on individuals require further steps to verify offenders beyond linking them to an IP address.

III. Generating meaning through the analysis of Internet Connection Records

Where public authorities need to resolve IP addresses, frequently the only additional data that will be available to assist them in doing so will be Internet Connection Records (ICRs). Internet Connection Records (ICRs) link not just the individual and their own IP address, but demonstrate what services they are connecting to or what IP address they are looking at and detail the connections made from a device to other online services. This is

[22] OFCOM n(15) 76.
[23] Stanley Burnton, *Report of the Interception of Communications Commissioner* (2016, HC 297) 21.
[24] Burnton n(23) Annex D.

done to allow investigators to pursue all lines of investigation, both known and unknown, and examine information which would have previously been unavailable.

a. Investigatory Powers Act 2016

The provisions in the Investigatory Powers Act 2016 enable existing capabilities to be maintained and enhanced by permitting more data to be utilised, and thereby provide the additional information necessary for them to be able to properly perform their investigative functions. In the context of IP address resolution, this takes the form of the inclusion of Internet Connection Records (ICRs). As per the provisions in the act, an ICR is record held by a CSP about the services to which a customer has connected to on the internet.[25] No single set of data constitutes an ICR; it will be different based on the service and the CSP concerned. This can include not only the IP address linked to a particular sender, but also what address they connected to, for how long, and when, what port numbers were associated, and an account reference.[26] This helps counteract the issues which arise due to the technical infrastructure wherein there are a limited amount of IP addresses and therefore they are difficult to link to individuals. Full ICR retention for analysis enables IP address resolution and thereby the powers of law enforcement to conduct investigations.

b. Internet Connection Record analysis: Processes and Problems

Despite the value to law enforcement in more accurately tracking and identifying online users, the inclusion of ICRs in the most recent Investigatory Powers Act was widely

[25] Home Office, *Operational Case for ICRs*, (4 November 2015) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504192/Operational_Case_for_the_Retention_of_Internet_Connection_Records_-_IP_Bill_introduction.pdf> accessed 8 Feb 2016, 7.
[26] *Ibid* 8.

criticised. Indeed, previous attempts to retain data akin to ICRs had consistently failed as such a requirement was seen to be disproportionately intrusive.[27] The fact that the information was useful was not seen to be sufficient to justify the obligation on CSPs or the additional interference with individual privacy which would result.[28] However, technological developments which allow for communications to occur via new applications coupled with the use of CGNs which make identifying individual users associated with previous categories of retained data difficult spurred the inclusion of ICRs in the legislation. The ability to access and interpret ICRs potentially enables the translation of data into real world investigative leads.[29] However, due to the highly revealing nature of the information generated by ICRs, there is a concomitant additional threat to privacy which results from the inclusion and analysis of this additional category of data.

IV. Analysing communications data using the 'request filter'

The 'request filter' seeks to improve the abilities of law enforcement to establish connections between different people and events by analysing substantial amounts of communications data,[30] and then filtering that information to only provide the relevant data to investigators. The communications data can then be assessed to determine links between suspects, provide exculpatory evidence, prove or disprove alibis, and so on. For example, if there had been multiple murders, this tool could be used to determine what

[27] Ian Brown Douwe Korff, 'Combined Papers No 1 & 2: technology development and its effect on privacy and law enforcement' (FIPR 2004) 13.
[28] Anderson n(2) 14.33.
[29] Joint Committee, Investigatory Power Bill Written Evidence National Crime Agency < http://www.nationalcrimeagency.gov.uk/publications/673-written-evidence-annexes-a-d/file> accessed 17 Feb 2017, 8.
[30] Communications data includes entity and events data as defined in Investigatory Powers Act 2016 s261(5). For an extended discussion of the 'request filter' see the author's article: Allison M Holmes, 'Automated Investigations: The Role of the 'request filter' in Communications Data Analysis' (2018) 2(2) J of Info Rights Practice & Policy, portions of which are included here.

devices were in the different locations at the relevant times, thereby narrowing down substantially the suspect pool for investigators. Without the 'request filter' investigators would have to approach each service provider individually, with a separate authorisation, and request the relevant data.[31] This traditional data request would disclose, not only the relevant data, but all other data that met the criteria of the application as well. The investigator would subsequently have to analyse all of this data to find the information needed. The 'request filter' therefore offers a way to simplify this complex search practice, and arguably limits the collateral intrusions into the data, to those which are necessary for the limited purposes of the investigation.

a. Draft Communications Bill 2012

It is apparent that this tool is of use to law enforcement and therefore easy to see why provisions for a 'request filter' have been a recurrent theme in discussions concerning communications data up to and including the passage of the Investigatory Powers Act 2016. For example, in 2008, a central government database of retained data was envisaged which would compile all the information into one easily searchable location. The communications data would be provided by CSPs but it would be stored on a Government owned and operated database.[32] This proposal was met with widespread criticism and was never implemented,[33] but the idea remained. In 2012, when considering the Draft Communications Bill, the 'request filter' was once again brought into the debate. The filter would similarly allow for the complex search of the retained data following a single request, but it would not be stored in a central database. 'So the

[31] Anderson n(2) 9.66.
[32] Joint Committee, *Draft Communications Data Bill* (2012-13, HL 79, HC 479) 5.
[33]Alan Travis and Richard Norton-Taylor, 'Private firm may track all email and calls' *The Guardian* (London 31 Dec 2008) https://www.theguardian.com/uk/2008/dec/31/privacy-civil-liberties accessed 2 Feb 2017.

same data is being stored about the same people and it is being stored in databases which are accessible to public authorities given powers under the Bill. The difference is that instead of one database there are many and they are privately owned'.[34] However, even though the databases would have been privately owned, the information held therein, including its format, data types, and retention length, would have still been dictated by the Government. This led some critics to argue that the provisions in the 2012 Bill were therefore a distinction without a difference; the filter could still be equated to a federated database.[35]

In order to access the 'request filter' as proposed by the Draft Communications Bill, a specified process needed to be followed. Namely, the investigator would submit a request for the filter to examine the data from multiple CSPs' databases and automatically analyse the returns, providing investigators with only the relevant data. The Secretary of State would control the filter but it would be for the CSPs to design and implement their own systems to accommodate the requests. Once this was completed, only the details of the devices active in both relevant locations would be sent back to the investigating officer. All other data would then be deleted. The general maintenance and design of this system was left to the individual CSPs as the databases required specialist skills to build, update, and maintain. This system arguably ensured that the issues present in the 2008 proposal, namely of placing the information in a central, government run database, were mitigated.

However, the proposed request system, like much of the ill-fated Draft Communications Bill, was heavily criticised. In spite of its value as a mechanism to diminish the amount

[34] Joint Committee n (32) 118.
[35] *Ibid.*

of data transferred to public authorities and thereby reduce levels of intrusion and protect privacy,[36] the proposals were rejected. Critics questioned the ability of the filter to truly provide an independent and impartial check on the processing of data when the system itself remained a function, delegated or otherwise, of the Home Secretary who was also responsible for issuing warrants and notices concerning the data.[37] Impartial governance of the system was necessary to ensure independence. Similarly, concerns were raised over the abilities enabled by the filters, particularly due to the scale and scope of the data involved. Within this system, data was collected from a wide variety of sources including internet, mobile, and traditional telephony and related to not only persons, but locations, and times as well. The potential abuse of the system could enable investigators to go on 'fishing expeditions'; the risk of this was not mitigated by the safeguards provided.

Demands were made for independent audits of the use of the filter by the Interception of Communications Commissioner (IOCCO) and more stringent requirements of necessity and proportionality before the filter could be used.[38] Similarly, 'the necessity and proportionality tests need to be applied not just to the individual data streams as supplied by CSPs but to the likely effect when they are assembled together'.[39] The ability of the data to create inferences about individuals was amplified by the comprehensive nature of the data collected and retained. This could not be neutralised by the fact that the data solely related to context rather than content of communications. Professor of media and communications, Robin Mansell, in her evidence to the Joint Committee examining the Draft Communication Bill, noted that 'Even if conventional content is separated from

[36]Home Office, *Draft Communications Data Bill Written Evidence* (2012-13) 242.
[37]Peter Sommer, *Draft Communications Data Bill Written Evidence* (2012-13) 526.
[38] Joint Committee n(32) 126.
[39] Sommer n (37) 533.

other forms of information which have meaning, the expansion of opportunities for authorities to draw inferences about citizens' intention or behaviour from patterns emerging from electronic tracing of their activities is growing exponentially'.[40]

These problems were further compounded by the lack of clarity concerning the implementation and transparency of the system used for the filtering. The algorithms used for filtering the data and provisions regarding their design and development were purposefully opaque. An element of transparency and scrutiny of the technical means would be required to ensure that the mechanism was being implemented appropriately. 'In the absence of clarity about this issue, authorities requesting and processing data will be continuously open to charges of biases'.[41] The problems highlighted in the development of the 'request filter' in the Draft Communications Bill remain under the provisions in the Investigatory Powers Act 2016 (IPA) to which the discussion now turns.

b. Investigatory Powers Act 2016

Despite the failure of the 2012 Bill, the need for a system for law enforcement to search, analyse, and connect relevant communications data to facilitate investigations and prevent collateral intrusions into personal data remained. Concurrently, criticisms of the data retention regime by the Courts mandated that greater safeguards were required to ensure these regimes limited the intrusions into privacy and personal data. These two factors informed the development of the 'request filter' in the IPA. Sections 67 to 69 consider the method, authorisations, and limitations of the 'request filter'. Principally, the method employed to use this system is the same as that under the 2012 Bill. Section

[40]Robin Mansell, *Draft Communications Data Bill Written Evidence* (2012-13) 399.
[41] *Ibid* 400.

67 provides for the powers to establish arrangements for the lawful, efficient, and effective obtaining and processing of communications data under the filter. The filter can be accessed by any listed public authority, when the test for granting access to that data has been met.[42] The filter has a limited function and can only process specified communications data as a result of a targeted communications data authorisation. A request is sent to the filter which acquires the data from the relevant CSPs and then discloses the data to those authorised to see it. The Home Office evidence for this provision attempted to distinguish it from its predecessors, noting that it would not enable those 'fishing expeditions' which were of concern in previous iterations. 'The 'request filter' is not a data mining tool or a search engine, as it can only operate on limited sets of authorised data using specified and authorised processing steps'.[43]

This authorisation process consists of an application made and approved by a designated senior officer of at least the rank of inspector.[44] This officer will consider the necessity and proportionality of the application and determine whether to grant access to the filter. In assessing this, the officer must confirm that the authorisation is necessary to obtain the data for a public protection purpose or for the purpose of a specific operation, and that the conduct is proportionate to the aims of the investigations.[45] Considerations of proportionality must take into account future evidential requirements including whether it will be possible to evidence records disclosed by the filter through subsequent communications data authorisations.[46]

[42] Investigatory Powers Act 2016 s 67; relevant public authorities include not only law enforcement but additional authorities from groups as wide ranging as HMRC to the Food Standards Agency.
[43] Home Office, *Joint Committee on the Draft Investigatory Powers Bill Written Evidence* (2016 IPB0146) 518.
[44] IPA n(42) s 67.
[45] IPA n(42) ss 68(4) & 68(5).
[46] Home Office, *Communications Data DRAFT Code of Practice* (June 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/724394

Additional safeguards are guaranteed in the Act to ensure that no communications data can be obtained or processed for any additional purposes outside of those for which the authorisation is given. Once the information has been provided to the relevant investigator, all additional data relating to the request will be deleted. The Act further puts provisions in place to allow for oversight of the process, along the lines of those requested in the 2012 Bill. Data must be made available to the Investigatory Powers Commissioner (IPC) for their functions of audit and oversight.[47] Any errors in the release of information processed by the filter must be reported to the IPC as well. Security of the system is required and provisions regarding the maintenance, testing, and development of the mechanism have also been included, however, there is very little explicit detail as to the format and structure provided.[48] These specifications are aimed at ensuring that the filter is subject to rigorous control.

However, many of the flaws inherent in the proposals for the 'request filter' in the 2012 Bill have been maintained in the IPA. The Secretary of State remains responsible for the establishment and maintenance of the system.[49] Similarly, the evidence offered by the Home Office that the authorisation procedure would prevent any misuse of data along the lines of the 'fishing expeditions' is not supported; this problem is compounded by the expansive nature of the data and relatively large pool of authorities who have access to the filter. 'Public authorities will have a permanent ability to access the 'request filter', which will make it an enticing and powerful tool that could be used for a broad range of statutory purposes. The ability to conduct the complex queries that the 'request filter'

/CCS207_CCS0618947544-001_Home_Office_Publication_of_Codes_CLIENT_PRINTIN....pdf> accessed 7 July 2018, 11.9.

[47] IPA n(42) s 69.

[48] IPA n(42) s 69(6).

[49] Home Office, *Joint Committee* n (43) 520.

will allow for could increase the temptation...to sift data in search of relationships and infer that consequences are meaningful'.[50] Similarly, the farming out of the retention systems, thereby removing it from a centralised Government control, does not necessarily mitigate the potential risks from the filter. This concern is exacerbated by the fact that there remains a lack of transparency both in the development of the filter and in the governance of the mechanism itself. Further, issues with oversight remain, as despite the inclusion of the audit and error powers for the IPC, there is no requirement of judicial approval in the authorisation process. The issues with the process, authorisation, and oversight provisions in the IPA are amplified by the nature of the data and the filter itself.

The 'request filter' is only able to meet its aims by sifting and analysing large quantities of communications data and interpreting that data to determine whether it satisfies the criteria of the requests. It can be broadly classified as a 'Big Data' tool, wherein Big Data refers to the use of large data sets for predictive analysis.[51] Big Data itself is a product of technological, analytical, and cultural elements. The technological aspect accounts for the development of systems and algorithms to gather, link, and compare data.[52] The analytical components then use the data compiled to draw inferences and establish patterns. The cultural elements inform these interpretations and form the foundation for the inferences which are obtained from the processing and analysis of the data. For the purposes of the 'request filter' here, the important elements are these analytical capabilities.

[50]Johanna Cherry, HC Debates vol 607, col 240 14 April 2016,.
[51] Kate Crawford and Jason Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) Boston C L R 93, 96.
[52] Kate Crawford, 'Critiquing Big Data: Politics, Ethics, Epistemology' (2014) 8 Intl J of Comm 1663.

V. Subsequent Analysis by Law Enforcement

Whilst requirements exist that must be satisfied prior to law enforcement being provided with access to relevant communications data, there are far fewer limits placed on the subsequent analysis and use to which that data is put. As opposed to the preceding sections which discuss the processing obligations placed on CSPs to analyse the data for law enforcement, the focus of this section is on the analysis and use of that data once it enters the possession of the public authority. As such, the rules governing this type of analysis do not fall under the remit of the investigatory powers instruments. Rather, in this type of data use, law enforcement agencies are bound by the Data Protection Act (DPA) 2018, Part 3.

Part 3 of the DPA was passed to give domestic effect to the provisions of Directive 2016/680 which governs the processing of personal data for law enforcement purposes, including the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[53] Under Part 3, law enforcement may process data so long as it is in accordance with law and constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interest of the natural person concerned.[54] Such processing must be for specific, explicit and legitimate law enforcement purposes. However, as long as the data was initially processed for such a

[53] Directive 2016/680/EC 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016) OJ L119. It is worth noting that under Article 6(a) of Protocol no 21 on the position of the United Kingdom…the United Kingdom is not bound by the rules which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 (Judicial cooperation in criminal matters) or Chapter 5 (police cooperation) of Title V of Part Three of the TFEU where the UK is not bound by the rules governing the form of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 TFEU (everyone has the right to the protection of personal data concerning them).
[54] Explanatory Notes to the Data Protection Act 2018 para 182.

legitimate purpose, it may then be processed for a different law enforcement purpose, so long as that additional processing is deemed necessary and proportionate.[55]

As such, law enforcement may continue to process data, beyond the scope of the original application for the data, so long as it still satisfies this law enforcement aim. The wording of the legal provisions surrounding this use is ambiguous and offers broad justifications for processing by law enforcement.[56] Whilst the general obligation that such downstream data processing meet basic legal requirements offers some safeguards for its future use, the lack of concise provisions governing this processing creates further concerns for individuals' rights. For instance, under this framework, communications data provided to authorities following a legitimate application for one investigation may be repurposed or used for a separate investigation, provided that the subsequent investigation still pursues a legitimate aim. When the information is shared in this manner, there are no provisions within the IPA which require that the subsequent processing be reauthorized. It is only under the DPA that such processing must be justified; however, such justification is an internal process and not subject to independent judicial scrutiny. Such concerns are compounded by the lack of a framework governing the sharing of the information between domestic law enforcement bodies.[57]

The result of this is that there exist very few controls or oversight over both the subsequent processing of communications data by the same law enforcement body and the sharing of that information between law enforcement bodies. This means that there is a significant risk that the accessed communications data will not be subject to the necessary safeguards which guarantee it complies with fundamental rights obligations.

---

[55] *Ibid* para 185.
[56]Catherine Jasserand, 'Law Enforcement access to personal data originally collected by private parties: Missing Data subjects' safeguards in directive 2016/680?' (2018) 34 Comp L & Sec Rev 154, 164.
[57] This is in contrast to international data sharing and transfer arrangements which may exist and are governed by the Data Protection Act 2018 ss 77 and 78.

Such a risk will become even more significant as law enforcement increases their data sharing capabilities. Notably, in the parliamentary report 'Policing for the Future' both the heads of the National Crime Agency and of the Metropolitan Police Force highlighted the need for increased data sharing as a policing priority.[58] Without additional guarantees regarding the use of this data, the risk to fundamental rights is significant.

One way to potentially mitigate the concerns which may arise from the use of this data would be to provide for increased information to be given to data subjects whose information is accessed and analysed by the police. However, under both the Directive and the DPA, these rights are limited. Data subjects whose information is processed for law enforcement purposes do not have the same subject access rights or rights to rectification, erasure, or restriction of processing that exist under the private processing provisions.[59] These rights may be restricted where informing the data subject would risk prejudicing the investigation.[60] Even once the investigation has finished and informing the data subject may no longer compromise the investigation, there is no requirement that the data subject be informed.[61]

The lack of notification for data subject is particularly problematic when the potential for further uses of the data is considered. Despite the ICO recognising that it is good practice to tell the individual as soon as possible once the risk of prejudice to the investigation has passed,[62] the Home Office has refused to incorporate any provisions regarding notification under the investigatory powers instruments. Indeed, the Home Office has gone so far as to cite the widespread processing of this data as a justification

[58] Home Affairs Committee, *Policing for the Future* (HC 2017-19, 515-X) paras 179-187.
[59] Data Protection Act 2018 s 43(3).
[60] Data Protection Act 2018 s 43(4).
[61] Jasserand n(56) 162.
[62] Information Commissioner's Office, 'Draft Data sharing code of practice' (2018) < https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf> 20.

for not providing notification. '[T]here are real challenges posed by the number of different authorities who are able to use these powers, and de-conflicting everyone involved in one investigation with all other investigations run by all public authorities, including the security and intelligence agencies, would be practically impossible'.[63] Far from justifying the lack of notification guarantees, such a statement by the Home Office highlights the widespread use of the data and the lack of sufficient safeguards. If it is not possible to tell who is utilising the data at any one time, then it is unlikely that there is any check that the powers are being exercised in a manner which complies with the requirements of necessity and proportionality. As such, the data may be analysed in a manner which is inconsistent with the rights of individuals; yet individuals themselves would not be aware of nor have any opportunity to challenge such analysis. Further, the oversight mechanisms which do exist, namely in the form of the Investigatory Powers Commissioner, do not have the remit to examine these downstream access procedures. There is no requirement that the IPC be notified of any subsequent uses to which the data is put. This type of analyses thereby presents a particular risk to individuals. Notification for individuals whose data is accessed and analysed would be a significant safeguard. The policy recommendations for incorporating this into future changes in the legislation will be explored in the concluding chapter.

VI. Applying Contextual Integrity to Communications Data Analysis

Having set out the mechanisms used for analysis, it is necessary to determine what the impact of these processes is on privacy. Relevant to this is the consideration of whether the analytical tools have altered the norms associated with data analysis for the purposes of criminal investigations. In this regard, it is important to recognise that it is not just

[63] Home Office. 'Investigatory Powers Act 2016 Consultation on the Government's Proposed Response to the ruling of the Court of Justice of the European Union on 21 December 2016' (November 2017).

technological capacities that are increasing, but the ability to generate meaningful data. As a result, the data gathered about people is more extensive, easier to aggregate, and able to be analysed in increasingly sophisticated and complex ways. As Helen Nissenbaum states, these powers 'make it possible for large troves of information to be reliably, efficiently, and meaningfully organised and accessed; to be effectively moved into massive aggregations and disaggregated into usable chunks; and to be transmitted to sites when needed'.[64]

The context in which this information is analysed is significant and contributes to the determination of whether the analysis is done in violation of informational norms. The context here is the defined social spheres relevant to the ICT system wherein these mechanisms operate. Changes in the information type, transmission principles, and actors involved in the analysis of the data represent challenges for the established informational norms.

With regard to the information types with which the analysis engages, the development of the technical capabilities have altered the nature of the information. Largely, these analysis mechanisms now operate in the digital environment. Removing information from traditional physical boundaries alters its nature. The amount of information which is generated in the digital sphere far exceeds that of its physical counterparts and can be aggregated. Whilst individual pieces of data may possess little revealing or relevant information, an assemblage of the data will be highly informative. When these assemblages are coupled with the large scale data sets derived through permissive data retention policies and advanced processing methods even more can be revealed. When

[64]Nissenbaum n(1) 37.

the data is merged together it generates further data and inferences, which can potentially be quite different from the original information.[65]

Similarly, the removal of the link to an individual from the process by breaking up information into communications data packets means that investigations using this information can no longer occur in the same manner. 'Digital footprints are neither observable nor readily identifiable as "belonging" to a particular person'.[66] Investigators cannot easily identify suspects using this information without some form of further analysis; the information provided through communications data requests is often incomplete. The data generated and retained is only done for law enforcement in limited instances. It is far more typical for the data to be generated for a commercial value and law enforcement use is secondary. The context of the data often changes as a result.

It is important to acknowledge that systems themselves are able to change the context of the data. This is significant as context is important in analysing data; meanings will change depending on the situation. Communications data can be used to draw meaningful inferences about peoples' connections to one another, about their movements, even about the strength of their relationships, but these interpretations need to be understood in a particular context to be persuasive. It is only within the known contexts that the analytic elements will be effective. Roger Clarke, posing his theory of dataveillance, described the importance of context for data. 'When the data are used outside their original context, the probability of misinterpreting them increases greatly. This is the reason why information privacy principles place such importance on relating

[65] Council of Europe, 'Study on the Human Rights Dimensions of Automated Data Processing Techniques (in particular Algorithms) and Possible Regulatory Implications' MSI-Net (2016) 06 rev 3 FINAL 13.
[66] Jennifer Daskal, 'The Un-Territoriality of Data' (2015-2016) 125 Yale L J 326, 331.

data to the purpose for which they are collected or used'.[67] When the data is removed from the context in which it was generated, processed, and collected, it means that the patterns and meanings derived are incomplete or lost.[68] Daskal similarly recognises the issue of context when data is collected *en masse*: 'the sheer quantity of data collected necessitates the use of presumptions as a basis for establishing identity. The vast quantity of data collected means that even a low error rate will yield large quantities of data associated with misidentified users'.[69]

Yet, in the processing of data sets, this change of context is often necessary for the system to be able to function. For example, in order for the 'request filter' to operate effectively, the data needs to be in a standardised format. This standardisation applies to the collection, analysis, and interpretation procedures. However, different business procedures and the lack of a proscribed format in the legislation mean that each CSP can retain the data in their own manner. This will necessarily result in the data being altered so that it can be processed in the format required by the 'request filter'. As the processing of this information is a secondary use for data collected by the CSPs, there will remain a question of who the analysts are truly accountable to in the development of the systems, their own company or the Government.[70] It is therefore important to recognise the issues which arise by altering the context of the data. As Crawford notes, 'Data are not generic. There is value to analysing data abstractions, yet retaining context remains critical, particularly for certain lines of inquiry. Context is hard to interpret at scale and even

[67] Roger Clarke, 'Information Technology and Dataveillance' (1988) 31(5) Comm of the ACM 498, 506.
[68] Busch refers to this concept as 'lossiness', 'that is, data collection and/or analysis may involve aggregation, case construction, or standardisation in such a way that certain aspects of the phenomena are lost.' Lawrence Busch, 'A Dozen Ways to Get Lost in Translation: Inherent Challenges in Large-Scale Data Sets' (2014) 8 Intl J of Comm 1727, 1732.
[69] Daskal n(66) 331.
[70] Susan Leigh Star, 'Simplification in Scientific work: An example from neuroscience research' (1983) 13 Social Studies of Science 205 notes the potential issues that arise from analysts being accountable to others in their analysis.

harder to manage when data are reduced to fit into a model'.[71] By allowing the context of the data to change, there is the risk that the potential for further profiling techniques which unnecessarily intrude into individual rights will be amplified.

The transmission principles which constrain the flow of information generated through the ICT system have similarly advanced alongside the development of analytical techniques. Typically, when users consent to having data collected and processed, they do so believing that the data will be used for specified purposes. Where individuals accept that there may be secondary uses to the data, such as its use by law enforcement, there would still be a violation of entrenched norms if the context and therefore the meaning of the data were changed by facilitating this use. Here this is evidenced by the way information is used and disseminated. Gillespie argues that, 'Algorithms are now a key logic governing the flows of information on which we depend, with the power to enable and assign meaningfulness, managing how information is perceived by users'.[72] These algorithms needn't be software; in a broad sense they can be those logics which transform input data into its desired output.[73] For example, law enforcement may use such technology for analysis which identifies relationships between individuals by sorting lists of telephone calls. In this manner, large lists of calls, their times, and durations will be input data which is then processed, typically utilising software, and turned into 'output' data which can be used in investigations.[74] Techniques such as this work because individuals' communication patterns tend to be regular, and following these patterns can provide valuable information about their network and contacts.[75]

[71]danah boyd Kate Crawford, 'Critical Questions for Big Data' (2012) 15 Information, Communication, and Society 663, 671.
[72] Gillespie n(7) 167.
[73] Gillespie n(7) 167.
[74] Brown and Korff n(27) 27.
[75] Brown n(5) 101.

Notably, in the analysis of information for investigative purposes, law enforcement are no longer the predominant actors. Rather, technological developments have resulted in CSPs being the primary mechanisms through which both the systems to analyse data are created and the information is actually assessed. This results in an organisational entity with powers to control and make determinations about an individual without being bound to the same standards as a State actor. In a way, this is necessary due to the technology. As McIntyre states, 'The growth of filtering, with its focus on intermediaries, is pragmatic in the sense that it frequently enrols actors who have knowledge and/or capacities for control which the government does not have'.[76] These actors have specialist skills and training which enable them to examine the information effectively.[77]

However, there are issues with using intermediaries to run what is effectively a law enforcement mechanism. For example, in their original form, analytical capabilities created by private actors likely had some specified business purpose as their primary aim. Frequently, the systems were originally built for security measures or targeted advertising. Solove notes that this type of development may be ill suited for achieving law enforcement aims.

> The problem, however, is that just because data mining might be effective for businesses trying to predict consumer behaviour, it isn't necessarily effective for government officials trying to predict who will engage in terrorism. A high level of accuracy is not essential when data mining is used by businesses to target marketing for consumers, because the cost of error to individuals is minimal.[78]

[76] TJ McIntyre, 'Intermediaries, Invisibility, and the Rule of Law' (March 2008) BILETA Conference Paper.
[77] Norris n(8) 211.
[78]Daniel Solove, *Nothing to Hide: The False Trade-off Between Privacy and Security* (Yale University Press 2011) 188.

While the provisions requiring the resolution of IP addresses, the retention of ICRs, and the creation and use of the 'request filter' are now set forth in statute, there are no specific technical requirements which set forth how these capabilities are to be created. It may remain up to the CSP to determine how to fulfil these aims. Therefore, in retaining and later processing the data, CSPs are essentially fulfilling a public interest objective but are not subject to the same limitations a public authority would be in fulfilling this role.

The technologies which are utilised for analysis alter traditional roles in other ways as well. Automated processing of data such as occurs through the 'request filter' removes the human element from the process. The role of large scale data sets allows these processes to fall under the category of a Big Data mechanism for these purposes. One of the promises of Big Data is that it allows for the removal of the subjective element in analysing and processing information and therefore allows for an interpretation based solely on 'facts'. Chris Anderson clearly stated this principle in 2008: 'Who knows why people do what they do? The point is that they do it, and we can track and measure it with unprecedented fidelity. With enough data, the numbers speak for themselves'.[79] When the ability for individuals to interpret the information is removed, proponents argue that the system itself can make informed analysis without the risk of bias. The power of the Big Data mechanisms is that their increasingly sophisticated techniques allow for the development of exact descriptive and predictive meanings from seemingly unrelated points of information.[80] This analysis therefore purportedly allows for an objective and purely informational mechanism. Within the 'request filter' this element is promoted as a safeguard; it keeps individual investigators from abusing the powers of the

[79] Chris Anderson, 'The End of Theory: The Data Deluge Makes the Scientific Method Obsolete' *Wired* (Science 23 June 2008) <https://www.wired.com/2008/06/pb-theory/> accessed 19 Jan 2017.
[80] Nissenbaum n(1) 42.

filter and making inferences about the data that are informed by their own biases. If the information can be filtered without the need for human inputs and interpretation, all that will be released will be impartial and factual results which the authorities can then use in their investigations.

However, it would be incorrect to imply that the human element can ever be fully removed from this type of data processing. All decisions, from the development of the system, to the request for access, incorporate a human element, whether it is in the design or the interpretation of the results. As such, 'data sets are not, and can never be, neutral and theory free repositories of information waiting to give up their secrets'.[81] This interpretation is critical to rebutting the presumption that automatic processing of data reduces the intrusions into private lives. As Lawrence Busch found: 'even the most apparently obvious results require (1) a degree of interpretation (in the formation of cases, in data collection, and analysis), and (2) the weaving of a master narrative around the data'.[82] When the data is interpreted, there is an implicit decision which favours a certain type of facts or elements over others. Within the 'request filter', this is manifest even in the forms and processes themselves; applicants can specify that they want to search for one type of information over another (e.g. mobile over internet) or examine data for certain locations but not others. To an extent this interpretation is necessary in order to ensure that the filter can function in an efficient manner. The data must be circumscribed at some stage, and the human input into which data to search makes this possible. However, it does mean that the promise that the data is objective and based on 'pure facts' cannot stand; if interpretation is incorporated into the decisions on what to search, certain facts will be weighted more heavily than others. Furthermore, removing

[81] Crawford n(51) 1668.
[82] Busch n(68) 1738.

the human element from the process removes a vital element of transparency and oversight. Feedback mechanisms can be utilised to determine the effectiveness of a process and its impact. In removing these mechanisms it is difficult to determine whether the processing is occurring in a fair and effective manner.[83]

The shift in investigative functions to CSPs and the increased automation of the system which removes the objective human element demonstrates a shift in the traditional roles associated with law enforcement analysis of personal information. Coupled with the changes in information types which result from technological developments which have changed the nature of the information and shifts in information flows as a result of analytical processes, the analysis of communications data which embodies these processes has changed the core elements of the informational norms and thereby breached contextual integrity.

VII. Conclusion

This chapter set out to determine the extent to which the communications data analysis methods pursue criminal justice aims, and the implications of these processes for privacy. The generation of data has increased exponentially through the incorporation of technologies into every aspect of modern life. Communications devices, whether they are telephonic or internet based contribute to this expanding data pool. Every communication which occurs via these devices leaves behind a digital trail of information. For law enforcement, that information can be a valuable resource in the investigation of crime. However, in order for it to provide the necessary information, the data must be analysed. This analysis allows for meaning to be derived. In the context of

[83] TJ McIntyre and Colin Scott, 'Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility' in Brownsword and Yeung (eds) *Regulating Technologies* (Hart 2008) 109, 116.

communications data analysis occurs through the resolution of IP Addresses, ICRs, the 'request filter', and subsequent use by law enforcement. The use of these analytical tools raises serious concerns for privacy as they represent a shift in the information types, transmission principles, and actors traditionally associated with analysing investigative information. The informational norms regarding data analysis have been altered in a manner which is inconsistent with the values of the system. This breaches contextual integrity and thereby privacy. The extent to which this breach, along with those identified in the retention and access processes, can be minimised through oversight protections under the law will now be discussed.

CHAPTER 6: OVERSIGHT

I. Introduction

Whilst the existence of privacy violations in the three preceding chapters is clear, it remains to be seen whether such intrusions can be offset through oversight mechanisms which enable them to strike an appropriate balance between privacy rights and law enforcement objectives. It is therefore necessary to examine the extant oversight regime in the investigatory powers mechanisms to ascertain whether it mitigates the privacy intrusions that result from the retention, access, and analysis of communications data. The significance of sufficient oversight has embodied much of the discourse surrounding the development of these powers. To this end, when introducing the Investigatory Powers Act, Theresa May promoted the Act as one which would 'establish world-leading oversight to govern an investigatory powers regime which is more open and transparent than anywhere else in the world'.[1] Such a claim is a direct result of the legal challenges to the investigatory powers regime, wherein the courts cited the lack of appropriate oversight as a key factor in holding that the interference with privacy resulting from these Acts was disproportionate. Following each of these cases, 'the law was amended to protect the surveillance powers of the police and the intelligence services, either by providing a necessary legal footing for those powers, or by bringing existing systems of authorisation and oversight into line with the demands of European law'.[2] This is by no

[1] Alan Travis Patrick Wintour and Ewen MacAskill, 'Theresa May unveils UK surveillance measures in wake of Snowden claims' *The Guardian* (4 Nov 2015) <https://www.theguardian.com/world/2015/nov/04/theresa-may-surveillance-measures-edward-snowden> accessed 20 Oct 2016.

[2] Benjamin Goold, 'Liberty and others v The United Kingdom: a new chance for another missed opportunity' (2009) P L 5. See the cases of Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications & Ors and Michael Seitlinger & Ors* [2014] 2 All ER; *Joined Cases C-203/15 Tele2 v Post-och telestyrelsen & C-698/15 Watson & Ors v Secretary of State for the Home Department* (2016) ECLI 970; *Malone v United Kingdom* App No 8691/79 (ECtHR, 2 Aug 1984);

means a phenomenon which is limited to the powers used in the United Kingdom; other jurisdictions similarly amended their communications data safeguards and oversight as a direct result of legal judgments.[3] The creation and strengthening of these oversight mechanisms through each subsequent iteration of the investigatory powers regime indicates the ability of these tools to permit these powers to withstand legal challenges. They are also promoted as critical instruments to ensure the rights of individuals who are subjected to the use of these powers. However, the nature of the communications data processes presents a challenge for oversight.

As a result, specialised supervisory bodies exist with responsibility for overseeing the collection, retention, access, and analysis of communications data.[4] This chapter analyses the role of these bodies in order to determine their effectiveness as measures which adequately balance privacy rights with the demands of the State. In order to do so, this chapter will be composed of six parts. Part I proceeds by first addressing the importance of oversight through a review of the relevant literature and case law which sets forth the significance of oversight as a check on the power of the state. Oversight ensures that the actions prescribed by the state comport with the necessary rule of law values crucial in a democratic society. The analysis will focus on how a balance can be struck between the aims of law enforcement and the fundamental privacy rights. Questions of oversight and accountability will help to dictate how that balance can be

Kennedy v United Kingdom App no 26839/05 (ECtHR, 18 May 2010); and *Liberty and Others v. the United Kingdom* App no 58234/00 (ECtHR, 1 July 2008) amongst others.

[3] See: Belgium, Draft Bill on data retention in the sector of telecommunications (Voorontwerp van wet betreffede het verzamelen en het bewaren van de gegevens in de sector van de elektronishe communicatie/Avant-project de loi relative à la collecte et à la conservation des données dans le secteur des communications électroniques) 2016; Germany, Law on data retention (Vorratdatenspeicherung) Art 113;

[4] To date there is little critical analysis of the role of these supervisory bodies in the field of law enforcement; discussion has largely been confined to their role in overseeing intelligence agencies.

struck and the appropriate standards which must be met when exercising powers concerning communications data.

Once the relevant criteria for effective oversight mechanisms which enshrine rule of law values and protections for fundamental rights are identified, discussion then turns to how oversight is currently administered in the investigatory powers instruments. Four key supervisory bodies will be examined. Part II will assess the role of the Information Commissioner in the communications data oversight process. Part III will focus on the (now defunct) office of the Interception of Communications Commissioner. Part IV examines the role of the Investigatory Powers Commissioner, created after the passage of the IPA. Part V will examine the judicial mechanisms for oversight in the form of the Investigatory Powers Tribunal. The aim of this analysis will be to identify how each body purports to meet the requirements necessary to protect fundamental rights as established by the case law of the ECtHR and CJEU. The shortcomings of each of these bodies are identified and critiqued with the aim of identifying areas in need of reform. This critique argues that the current oversight regime is insufficient to protect privacy in the context of communications data retained under ICT systems. Finally, Part VI will establish that the violation of contextual integrity in the ICT system resulting from the retention, access, and analysis of communications data is not diminished by the existing oversight and safeguards. Prescriptive measures are needed to amend the oversight provisions as they concern communications data in order to better reflect these changes and ensure that the vital privacy interest violated by the investigatory powers instruments are protected.

II. The importance of oversight for the rule of law

The use of communications data by law enforcement demonstrates an expansive governmental power and must therefore be subject to the rule of law lest it violate fundamental rights disproportionately when seeking to promote the aims of a democratic society. In order for these powers to accord with the rule of law certain requirements must be met. Any measures which interfere with fundamental rights must be assessed against the principles of legality, necessity, and proportionality. To ensure these provisions comport with the principle of legality, the legal rules justifying the interference must be accessible, clear, and precise, as discussed by the UN Special Rapporteur on Privacy, Joseph Cannatacci.[5] Similarly, the interferences must be necessary; there must be limits on the use of discretion or 'exceptionalism' in the use of these powers by state authorities.[6] Notably, for the purposes of this chapter, Bigo et al argue that 'there must be mechanisms of accountability and supervision by an independent judiciary at the heart of the system'.[7] Any measures that interfere with these rights must further be balanced against the alleged benefit that can be derived from the interference; in other words, they must be proportionate. In the absence of such safeguards, the collection and processing of communications data will be fundamentally contrary to the rule of law and incompatible with core fundamental rights principles. In order to assess whether the oversight mechanisms employed for communications data meet these standards, it is necessary to first establish the extent to which these powers satisfy these requirements of legality, necessity, and proportionality. The extent to which

[5] Joseph Cannatacci, 'Report of the Special Rapporteur on the Right to Privacy' (UN General Assembly 30 Aug 2016) A/71/368, 10.
[6] Guillermo O'Donnell, 'The Quality of Democracy: Why the Rule of Law Matters' (2004) 15 J of Democracy 4, 31.
[7] Didier Bigo Sergio Carrera et al, 'National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU Law' (2013) European Parliament DG for Internal Policies PE 493.032, 31.

the current mechanisms satisfy these requirements will help determine the effectiveness of the current oversight and areas for future development.

a. Legality

For an interference with fundamental rights to be justified it must be found to be in accordance with law. As such, any provisions which enable the communications data powers discussed in this thesis must be adequately provided for in law. The law must be accessible and foreseeable, thereby enabling the individual to identify, with sufficient precision, when their conduct might be caught by the regulation. With regard to surveillance, precedent requires that, 'The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures'.[8] This does not require that individuals be provided with detailed information about the surveillance regimes utilised to capture their data for law enforcement purposes. Where providing individuals with information might frustrate the intended purpose of the legislation, (i.e. by giving suspects detailed information on when their communications data may be targeted), disclosure may be limited to ensure the aims of national security and the prevention and detection of crime.[9]

[8] See: *Malone v United Kingdom* App No 8691/79 (ECtHR, 2 Aug 1984) paras 66-68; *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000) para 55; *Amann v Switzerland* App no 27798/95 (ECtHR, 16 Feb 2000)*; Kruslin v France* App no 11801/85 (ECtHR, 24 April 1990) para 27; *Lambert v France* App no 46043/14 (ECtHR, 24 June 2014) para 23; *Perry v United Kingdom* App no 63737/00 (ECtHR, 17 June 2003) para 45; *Dumitru Popescu v Romania (no 2)* App no 71525/01 (ECtHR, 26 April 2007) para 61; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* App no 62540/00 (ECtHR, 28 June 2007) para 71; *Liberty and Others v. the United Kingdom* App no 58234/00 (ECtHR, 1 July 2008) para 59; *Szabo & Vissy v Hungary* App no 37138/14 (ECtHR, 12 Jan 2016) para 59.

[9] See *Szabo & Vissy v Hungary* App no 37138/14 (ECtHR, 12 Jan 2016) para 62: 'Foreseeability in the special context of secret measures of surveillance,…, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly'.

Established case law requires that such mechanisms which permit interferences with fundamental rights by enabling the collection and processing of information must be governed by precise rules pertaining to the scope and application of the measures, as well as safeguards regarding access, usage, procedures, and destruction.[10] However, the requirements for investigatory measures to be 'in accordance with law' in line with the relevant jurisprudence does not require the precise rules and safeguards to be explicitly set forth in statute. The Courts have accepted that the Executive has discretion to provide for these elements in secondary instruments rather than the substantive law.[11] Administrative orders, Codes of Practice, and guidance are accepted mechanisms for ensuring these powers are 'in accordance with law'.[12]

In accepting these instruments as sufficient, the Court will look at the availability of the information to the public and the process by which it came in to force. The ability of individuals to access information about the procedures which may be applied to them is crucial for the rule of law; individuals must know what laws they are bound by and when they may fall foul of those laws. The Court will also look to the effect that the instrument has on governing the actions of the relevant public authority. In the UK, the validity of the Codes of Practice relating to the investigatory powers regime was called in to question in *Kennedy v United Kingdom*. Therein, the Court held that the Codes of Practice under RIPA were sufficient to meet the requirements of foreseeability.[13] The current Codes of Practice under the investigatory powers regime are likely to similarly

[10] *Kruslin v France* App no 11801/85 (ECtHR, 24 April 1990) paras 33 and 35; *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000) para 55; *Weber & Saravia v Germany* App no 54394/00 (ECtHR, 29 June 2006); *Liberty and Others v. the United Kingdom* App no 58234/00 (ECtHR, 1 July 2008) paras 62-63; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications & Ors and Michael Seitlinger & Ors* [2014] 2 All ER para 99.
[11] *Malone* n(8) para 68.
[12] *Liberty* n(8) para 61.
[13] *Kennedy v United Kingdom* App no 26839/05 (ECtHR, 18 May 2010) para 157.

satisfy these requirements. Thus, provided the Codes give adequate indication of the scope and powers of the public authorities and provide for specific safeguards, they will satisfy the requirement that the communications data powers are 'in accordance with law' for the purposes of justifying an interference with fundamental rights.

b. Necessary in a democratic society

Regardless of the legality of the provisions regarding communications data, the processing and collection of such information will violate fundamental rights where the powers are not deemed necessary. The ruling in the case of *S and Marper v United Kingdom* requires that in cases where the interference is with individuals' personal data, and involves the use of potential cutting-edge technologies to invade privacy, the criteria of 'necessary in a democratic society' must be interpreted as strict necessity.[14] Strict necessity requires that the power is necessary for 'safeguarding the democratic institutions, and moreover,..., for the obtaining of vital intelligence'.[15] In the context of communications data, the case of *Tele2 Sverige* confirmed that national legislation must abide by the requirements of strict necessity to justify any interference with privacy.[16] Similarly, any data collection policies, undertaken through secret means, which concern persons not suspected of involvement in a specific crime or posing a threat must be subject to a strict necessity test to justify the interference with a fundamental right.[17]

Concomitant with the requirement that the powers be strictly necessary is the condition that they be proportionate to the aim to be achieved. The requirement of proportionality

[14] *S and Marper v United Kingdom* App No 30562/04 and 30566/04 (ECtHR, 4 Dec 2008) para 73.
[15] *Ibid*
[16] *Joined Cases C-203/15 Tele2 v Post-och telestyrelsen & C-698/15 Watson & Ors v Secretary of State for the Home Department* (2016) ECLI 970 para 107.
[17] Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' CON (1985) 108.

is particularly important when considering the communications data tools as they indiscriminately relate to large swathes of the population in the absence of any reasonable suspicion that they have been involved in a crime. Settled case law requires that due regard must be had for the principle of proportionality when derogating from and limiting fundamental rights.[18]

In determining whether a provision goes beyond what is strictly necessary, the courts will take several factors into account, including the existence of effective safeguards and guarantees against abuse. Such an assessment will examine the existence of judicial scrutiny, the independence of authorisation procedures, and the affected parties' rights to remedy and redress for alleged violations of the right. As a general principle, interference with individuals' rights should be assured by independent judicial scrutiny. 'The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law'.[19] It is this independent review which ensures that these powers are not abused and provides public trust in the system. In the absence of such a check on the powers of authorised bodies, questions will arise over the validity and proportionality of their actions. Such a level of scrutiny is accepted as necessary in spite of arguments that accessing communications data is less intrusive than its content counterpart. As Joseph Cannatacci succinctly states, 'Legislation that does not lay down clear and precise rules governing access even to metadata, and legislation that does not provide for "effective judicial protection", cannot

[18] C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi and Satamedia* (C-73/07) [2008] ECLI 727 para 56; C-92/09 and 93/09 *Volker und Markus Schecke and Eifert* [2010] ECLI 662 para 77; Case C-362/14 *Max Schrems v Data Protection* Commissioner (2015) ECLI 650 para 92-96; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications & Ors and Michael Seitlinger & Ors* [2014] 2 All ER para 52.
[19] C-194/84 *Partie écologiste "Les Verts" v European Parliament* [1988] ECLI 94 para 23; C-224/84 *Johnston* [1986] ECR 1651 paras 18 and 19; and Case C-362/14 *Max Schrems v Data Protection* Commissioner (2015) ECLI 650 para 95.

be necessary or proportionate to the legitimate aims of crime prevention or national security'.[20]

Yet, these requirements are not absolute, and the Court can find that a combination of mechanisms, short of formal judicial control, is acceptable, in particular if 'initial control is affected by an official qualified for judicial office'.[21] Where authorisations of the processes are approved by a non-judicial body, the Court must be assured that said body is independent of both the Government and the interested parties.[22] In determining whether the communications data regime meets human rights standards, it is necessary therefore to examine the existing bodies and their powers to determine the extent to which they comply with the rule of law. The discussion will now turn to analysing the bodies involved in supervising and overseeing the communications data regime, beginning with the Information Commissioner.

III. The oversight role of the Information Commissioner: technical requirements and data security

The Information Commissioner has a limited remit with regard to communications data, focusing principally on technical capabilities and enforcement of retention notices. As such, the discussion of her powers herein will be brief.

a. Function and Powers of the Information Commissioner

With regards to communications data, the Information Commissioner has oversight power regarding retention notices and the storage and use of the retained data. These powers only relate to the handling of the data once the notice has been issued and the

[20] Cannatacci n(5) 23.
[21] *Weber* n(10) para 115; *Kennedy v UK* n(13).
[22] *S and Marper* n(14) para 77.

data retained; the ICO does not have access to what is retained nor a role in determining what should be retained.[23] Once a CSP is issued with a retention notice, this, along with any other relevant information, will be communicated to the ICO. The ICO is then responsible for overseeing the security, integrity, and destruction of retained data.[24] The ICO has audit powers of these technical system requirements and may issue reports on how the CSPs are complying with their obligations.

However, it is important to note that the publication of information concerning inspections of retention notices by the ICO will not occur if the confidentiality of those notices will be compromised by publication. As a result, these reports will be redacted to protect the identity of companies which are subject to a notice.[25] The inability of the ICO to fully publish the results of their inspection raises questions over transparency and accountability. It is an instance where the Home Office is perceived to be 'marking their own work' by obfuscating the results of the ICO audits, as they can dictate what elements of the reports are subsequently disclosed. The ICO further suffers from a lack of statutory powers regarding retention notices and compliance requirements.

In addition to her role in overseeing the integrity, security, and destruction requirements of data retained by CSPs, the ICO has additional powers under the Data Protection Act 2018 (DPA) with regard to the subsequent processing of the data. Her competencies with regard to law enforcement processing may be engaged in two ways. First, when data is collected and processed for law enforcement.[26] Second, when the data is initially

[23] European Union Agency for Fundamental Rights (FRA), 'Surveillance by Intelligence services: fundamental rights, safeguards, and remedies' (2017) Vol 2, 82.
[24] Home Office, *Retention of Communications Data Code of Practice* (March 2015) Chapter 7.
[25] *Ibid.*
[26] Directive 2016/680/EC 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016) OJ L119, Recital 11.

collected for a non-law enforcement purpose and then further processed by law enforcement authorities.[27] Both scenarios require that the law enforcement authorities adhere to the requirements of Part 3 of the DPA.

The provisions of this part of the Act apply to all competent authorities who will, as part of their functions, process personal data for law enforcement purposes.[28] These purposes include the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[29] In utilising data in the fulfilment of these purposes, the authorities must comply with six data protection principles which relate to the fair processing of data.[30] Authorities must implement the appropriate measures to comply with these principles, maintain documentation as to how they have done so, and where appropriate, appoint data protection officers and/or implement measures with regard to data protection by design and data protection by default. The ICO does not play a direct role in instituting these procedures at the level of the public authority but offers guidance for these organisations in doing so.

The ICO has more direct powers where data breaches have occurred in the discharge of these law enforcement functions. Yet these are to some extent limited. As opposed to data breaches by private organisations which must be reported to the ICO, data breaches resulting from law enforcement processing must only be communicated to the commissioner where there is a likely risk to the rights and freedoms of individuals if left unaddressed.[31] If the authority fails to notify the ICO of a breach when required to do so they can be subject to a fine. However, there are areas of overlap between this

[27] Regulation 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) (2016) OJ L 119/1 Recital 19.
[28] Data Protection Act 2018 Schedule 7.
[29] *Ibid* s 31.
[30] *Ibid* ss 35-40.
[31] *Ibid* s 67.

requirement and those under the Investigatory Powers Act 2016. Notably, where a data breach may also be classed as a relevant error under the IPA, the requirements governing the communication of a personal data breach do not apply.[32] Where this is the case, errors must only be reported to the Investigatory Powers Commissioner (discussed below) who will then consider whether they have resulted in any errors which should then be reported to the ICO. Further, no disclosures can be made to the ICO where doing so would be prohibited under the IPA.[33] As a result, the powers of the ICO with regard to data provisions under the IPA are considerably more limited than her powers under the DPA. The restrictions on the ICO with regard to the powers under the IPA are, to some extent, then covered by the IPC. However, this remains insufficient to effectively guarantee the rights of individuals whose data is processed.

b. Criticisms of the powers of the Information Commissioner

One of the primary powers of the ICO rests in her ability to audit companies' data storage and security infrastructure. Under the early investigatory powers instruments, the Commissioner lacked specific audit powers.[34] However, following the passage of the IPA 2016, the Information Commissioner is now imbued with powers to audit requirements or restrictions imposed regarding communications data.[35] This has placed on statutory footing the ability of the Commissioner with regard to oversight of the integrity, security, and destruction of data retained under a notice.

Yet even when the Commissioner is able to audit the relevant functions of the CSP, much will actually depend on the content of the retention notice. The ICO can only audit the

[32] *Ibid* s 108(6).
[33] *Ibid* s 131(2).
[34] Home Office, *Acquisition and Disclosure of Communications Data and Retention of Communications Data Codes of Practice* (March 2015).
[35] Investigatory Powers Act 2016 s 244.

mechanisms of retention provided for in the notice. 'This means that the provisions of the retention code itself and the notice are of crucial importance to delivering the intended safeguards and the Commissioner's role in ensuring these are applied in practice'.[36] The Commissioner's inability to consult on these notices prior to their issuance mean her power is circumscribed. There is no requirement that the ICO be consulted on the contents or specifications of a notice however, they may be consulted by the Home Office if that notice is later subjected to review, variation, or revocation.[37] In addition, even when an audit of the technical requirements imposed by a retention notice is undertaken by the ICO, much will depend on the cooperation of the CSP. 'The requirement to have the consent of the data controller before conducting an inspection limits proactive oversight and the deterrent effect of possible inspection in areas where there may be real risks to compliance'.[38] The Commissioner would be better equipped to deal with issues regarding data retention if she was empowered to compel audits for CSPs. Her inability to do so represents 'a significant limitation on her ability to investigate, identify problems, and prevent breaches'.[39]

Moreover, the Information Commissioner is not consulted when measures that engage areas within her competence concerning communications data are brought before Parliament. This reduces her ability to ensure adequate safeguards exist within the legislation and promote privacy and data protection. Indeed, the Commissioner's office notes that the recommendations that she be consulted in the legislative process were

[36] *Ibid*
[37] Home Office, *Communications Data DRAFT Code of Practice* (June 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/724394/CCS207_CCS0618947544-001_Home_Office_Publication_of_Codes_CLIENT_PRINTIN....pdf> accessed 7 July 2018 para 18.5.
[38] House of Lords, *Surveillance: Citizens and the State* (2009, HL 18) <www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1807.htm> accessed on 25 April 2015.
[39] House of Commons Justice Committee, 'The functions, powers and resources of the Information Commissioner' (9th Report of Session 2012-13 edn House of Commons 2013).

'founded on the need to ensure that as relevant developments occur in future, data protection and privacy interests are considered at the very earliest stage'.[40] Failing to take these concerns into consideration during the drafting of legislation and secondary instruments means that they are not afforded the necessary protections.

Additionally, even when the privacy and data protection concerns of the ICO are taken into account, such consideration may not occur until well into the process, as it is unlikely the primary goal of the legislation is the protection of such interests. 'This can have the potential result of safeguards being implemented at a late stage as a compromise, and possibly more expensive, inadequate solutions'.[41] In addition, the Commissioner should be allowed to scrutinise the legislation post enactment, following a report on its deployment, the supposed value of any data retained, and the continued necessity of the measures.[42] The limited powers of the Information Commissioner with regard to audits and consultation diminish its efficacy as an oversight mechanism for the investigatory powers instruments. Not only does the minimal role of the Commissioner call into question whether adequate safeguards are considered in the implementation of policy, but also whether such safeguards, when included in legislation, can be satisfactorily enforced.

IV. The role of the Interception of Communications Commissioner (IOCC): overseeing communications data use

Whilst the Information Commissioner plays a relatively minor role in the oversight of communications data, overseeing only technical data retention capabilities, the Interception of Communications Commissioner (IOCC) oversaw much broader areas of

[40] House of Lords n(38).
[41] *Ibid.*
[42] Christopher Graham, Liverpool John Moore's Roscoe Lecture (12 Jan 2015)

access and analysis of the data retained. Before turning to further discussion of the IOCC however it is crucial to note that this Commissioner and his relevant duties have been overtaken by the Investigatory Powers Commissioner (IPC). The following section will focus on the role of the Investigatory Powers Commissioner; but it is necessary to first discuss the Interception of Communications Commissioner as, until 2017, the IOCC was the principal oversight body for the investigatory powers instruments.

a. Functions and Powers of the Interception of Communications Commissioner

The Interception of Communications Commissioner was the primary supervisory authority for the investigatory powers instruments since the office first received statutory footing under the Interception of Communications Act 1985.[43] Under the 1985 Act, the Commissioner acted as an *ex poste* review mechanism for authorisations. Former Commissioner Sir Thomas Bingham described the role as 'largely retrospective, to check that warrants have not been issued in contravention of the Act and that appropriate procedures were followed'.[44] The responsibility for retroactive review continued under RIPA and DRIPA. As such, the IOCC worked to hold those public authorities exercising RIPA powers to account and to improve compliance and confidence by means of scrutiny.[45]

The IOCC was provided with resources to satisfy the aim of increasing this scrutiny and compliance.[46] With regard to communications data, the IOCC worked with both CSPs and the public authorities to ensure that appropriate procedures were in place. As such,

[43] Interception of Communications Act 1985 s 8 required a Commissioner be appointed to oversee the use of the powers under the Act.
[44] Thomas Bingham, 'Report of the Interception of Communications Commissioner' (1992).
[45] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (Stationary Office 2015) 109.
[46] This included a staff and a secretariat who assisted in the inspections of public authorities.

the staff of the IOCCO required technical facilities and training, and the Secretary of State was required to consult with the Commissioner to ensure that these resources were adequately provided.[47] In order to fulfil the objectives of the Commissioner's office, the IOCCO staff were pulled from a wide range of backgrounds, covering legal, investigative, analytical, and forensic telecommunications.[48] However, as will be discussed, the qualifications of the members of the IOCCO could not necessarily overcome wider issues with regard to limited powers and resources. In order to adequately assess the effectiveness of the oversight provided by the IOCC, it is first necessary to define the extent of their powers.

The IOCC had several powers with regard to communications data. Principally, the IOCC carried out inspections of public authorities. In doing so, they would audit the records of these authorities; it is worth noting that the powers of the IOCC to audit extended to all public authorities with RIPA powers, not just law enforcement.[49] Inspections of the larger users, such as police forces, occurred over three to four days and were conducted by at least two inspectors.[50] Smaller authorities were generally inspected in one day by a single inspector. Due to the large number of communications data requests (over 750,000 in 2015), it was not practical for the IOCCO to audit all applications; therefore the audits occurred largely through sampling. To assess the applications for communications data the IOCCO examined the standards of necessity and proportionality utilised by public authorities.

For these standards to be considered adequate, applicants requesting access to communications data needed to provide a description of the perceived value of the data

[47] Regulation of Investigatory Powers Act 2000 s 57(5).
[48] Stanley Burnton, *Report of the Interception of Communications Commissioner* (2016, HC 297) para 2.6.
[49] *Ibid* para 7.41.
[50] *Ibid.*

for their investigation. This normally would include an explanation of the crime under investigation, the suspect (or witness or victim) whose information they were seeking, and the relevant phone or communications address.[51] The majority of the applications were put forward for preventing or detecting crime and/or disorder.[52] These applications further required that the measures be proportionate and limit collateral intrusion. Consideration of these requirements must have been made before an authorisation was granted by the designated person, usually a senior officer. The IOCCO in assessing whether the public authority adequately considered these elements would look to the 'operational conduct carried out, or put another way, the downstream use of the material acquired'.[53] Such an analysis looked at the way the material was used/analysed; whether it was used for the intended or a secondary purpose; what the actual, as opposed to perceived, interference with fundamental rights, including privacy, was; and whether an error or breach ultimately resulted from the use of the data.

Once the inspection was complete, the IOCCO issued inspection reports which highlighted issues to be addressed by public authorities in future applications for data. Such inspection reports would come with recommendations on good practice to help the authorisations comply in future. The IOCCO had no ability to impose sanctions on those authorities who had failed their inspections, nor could they remove the powers of offending authorities to access communications data until they complied with their recommendations. Public authorities were required to have regard for the provisions which set forth the specific requirements concerning authorisations for access to

[51] *Ibid.*
[52] 85.8% of communications data sought in 2015 was for this purpose. The other data was sought for preventing death, injury or damage to a person's physical or mental health (8%) or in the interest of national security (6%).
[53] Burnton n(48) para 7.46.

communications data, but there were no civil nor criminal liabilities for failing to do so.[54] The inability of the IOCC to impose sanctions or guarantee credible enforcement limited the potential effectiveness of the oversight, particularly with regard to criminal investigations. As Jon Michaels notes, 'absent the credible threat than an investigation will be for naught if it is shown to have been conducted in an extra-legal fashion, individuals may well be emboldened to act with less regard for legal formalities'.[55] In this regard, their power was largely advisory and there was little clarity on how pervasive non-compliance by a public authority could be mitigated.

Despite the inability to issue sanctions where data was accessed in a manner contrary to the relevant guidance and Codes of Practice, the IOCCO did retain responsibility for errors and breaches concerning communications data. This responsibility was confined to those errors which were identified by public authorities and subsequently reported to the IOCCO. The IOCCO would review such errors and assess any mitigating actions that had subsequently been put in place.[56] The provisions concerning error reporting were crucial for oversight. Errors in requests for access can potentially lead to individuals being wrongly targeted and have severe impacts on individual rights. Take the example of IP addresses. These are often used to identify individuals who have accessed illicit materials online and can be the only line of inquiry into serious offences such as online child sexual exploitation. However, this category of information is also the most prone to error, as requesting applications frequently fail to specify the correct date or time.[57] This has the adverse effect of individuals being wrongly identified and

[54] See RIPA s 72 and Burnton n(48).
[55] Jon Michaels, 'All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror' (2008) 96 Cal L R 901, 926. This similarly has implications for the admissibility of evidence at trial. Evidence obtained on foot of a faulty access authorisation may still be allowed in subsequent prosecution.
[56] Anderson n(45) para 6.101.
[57] Burnton n(48) para 7.85.

can have potentially devastating consequences. Despite the potentially serious impact on individuals, there was no explicit requirement that an individual be informed of this error.

However, the IOCC did have discretionary power to inform individuals of errors and breaches concerning the use of the communications data where such errors were considered 'serious' and were a result of 'wilful and reckless failures' of public authorities to abide by the requirements of the relevant Codes of Practice.[58] No guidance existed as to what might enable an error to fall under this category. Circumstances in which a breach could be classified as serious included: technical errors by CSPs which led to a significant number of erroneous disclosures; errors where the public authority subsequently initiated a course of action impacting on an individual as a result of the information; and errors which resulted in the disclosure of a large volume of data or data that was considered sensitive.[59] Where the Commissioner was satisfied that such an error occurred, he *could* inform the individual of the suspected unlawful behaviour.[60] There was no positive obligation on the Commissioner to inform individuals; the decision was left to his discretion. The lack of a requirement for information when an individual was impacted by erroneous actions of a public authority was a significant gap in the oversight regime, and one which remains under the IPCO which will be discussed below.

Upon completion of the aforementioned audits which examined the use of and access to communications data, the Commissioner issued an annual report to be laid before Parliament. These reports served to provide evidence of the legitimate use of these powers and call attention to any ways the RIPA powers were being abused. The existence of this annual reporting system was used to support the argument that the IOCC

[58] Burnton n(48) para 7.92.
[59] Interview with Robin Wevell, Head of the IOCCO, Home Office (June 2016)
[60] Home Office, *Retention* n(24) para 8.3.

is a sufficient safeguard for the use of investigatory powers, an argument with which the ECtHR agreed in the case of *Kennedy v United Kingdom.* Therein it was held that,

> The Court considers that the Commissioner's role in ensuring that the provisions of RIPA and the Code are observed and applied correctly is of particular value and his [then] biannual review of a random selection of specific cases...provides an important control of the activities of the interception agencies and of the Secretary of State himself.[61]

However, despite the initial judicial acceptance of the functions and powers of the IOCC as a safeguard against abuse, technological advances and subsequent case law called into question this determination. The IOCC was no longer a sufficient safeguard for the communications data activities under the investigatory powers regime.

b. Criticisms of the Interception of Communications Commissioner

The IOCC was subject to limitations which greatly diminished his ability to function as an effective and efficient oversight mechanism. In order to determine whether the IOCC provided sufficient oversight to justify privacy interferences occasioned by access to communications data, it is necessary to examine these limitations, before turning to discussion of how these issues were addressed in the creation of the new office of the Investigatory Powers Commissioner.

In assessing the independence of the IOCC, it is necessary to first examine the appointment and financial provisions governing the office. Case law has determined that the manner of appointment, duration of term of office, and guarantees against outside

[61] *Kennedy* n(13) para 166.

pressures will be crucial factors in determining whether the body is truly independent.[62] For the IOCC, the Commissioner was appointed by the Prime Minister on recommendation of the Home Secretary. This created a relationship with, and a potential dependency on, the Executive. Further, budget and technical facilities were subject to Treasury approval.[63] This provided Government control over crucial elements for the body, including staffing, funding, and facilities. The Home Secretary remained responsible for recommending the appropriate resources to be allocated by Treasury in this regard. In essence, the Home Secretary was responsible for funding a body which was responsible for reviewing the exercise of her powers.[64] This considerably weakened the independence of the IOCCO; it is inappropriate for the Home Secretary to determine the budget for a body who is responsible for overseeing their own performance. Close relationships between the Government and the supervisory agency, whilst not explicitly prohibited, must be circumscribed by clear legislative provisions.[65]

Further, practical elements concerning the functioning of the IOCCO conflicted with its independence. The offices of the IOCC were found in the Home Office and inspectors noted that there was often indirect pressure applied to ensure that their reports reflected perceived policy aims.[66] This raised concerns over the perception of independence for the body. The body must not only be independent; it must also appear independent to ensure public trust.[67] Such limitations to independence, whether perceived or otherwise,

---

[62] *Campbell and Fell v United Kingdom* App nos 7189/77 and 7878/77 (ECtHR, 28 June 1984) para 78.
[63]RIPA s 57(5).
[64] Burnton n(48) para 5.17.
[65] For example, the Court in the case of *Weber* n(10) examined secret surveillance measures under the German G10 Act. This Act provides for a stringent oversight regime which requires accountability not just to the Government but also to Parliament and an independent Commission. The relevant minister must report to these bodies before the surveillance measures are authorised. Whilst discussion of independence of the IOCCO, challenged in the case of *Liberty* n(8), did not comment directly on this issue, the argument can be made that the repeated references to the aforementioned oversight regime discussed in *Weber* offers an implicit criticism of the UK system.
[66] Interview with Robin Wevell, Head of the IOCCO, Home Office (June 2016).
[67] European Union Agency for Fundamental Rights n(23) 74.

raised questions over the Commissioner's capabilities. Independence needs to be clear; even the perception of government interference casts suspicion on the ability of the IOCC to function as an effective supervisory agent. The inability to fully separate the IOCC from the Government supported the argument that the IOCC was insufficiently independent to satisfy necessary human rights requirements. Conflicts arose due to the role of the IOCC as both a department of the Home Office and a regulator of it.

In addition to questions of independence, the IOCC had relatively limited powers. As noted above, the IOCC was entitled to make reports concerning the acquisition of communications data by public authorities and any errors or abuses therein. This brought an important element of transparency to the authorisation process and acted as a check that these powers were not being used unnecessarily or disproportionately. However, in auditing the communications data authorisations made by public authorities, there was a risk of regulatory capture. JUSTICE, in their report 'Freedom from Suspicion' noted that testimony of the IOCC indicated that the Commissioner at the time strongly identified with the work of public authorities in a manner that was inappropriate for a supervisory agent charged with the review of the decisions of those bodies.[68]

The results of the inspections which determined errors were compiled into an annual report laid before Parliament. However, the Prime Minister, on advice of the Home Secretary, retained the ability to edit these reports prior to publication to remove potentially 'sensitive' material. This was criticised as amounting to a *de facto* veto power over the contents of the Commissioner's reports.[69] Additionally, these reports were not comprehensive; they covered a sample of authorisations for communications data. Even

[68] JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age* (2011) < https://2bquk8cdew6192tsu41lay8t-wpengine.netdna-ssl.com/wp-content/uploads/2015/01/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf> accessed 25 Nov 2015.
[69] Burnton n(48).

if common errors or abuses of powers were determined which might be of public concern, the IOCC could not launch broader inquiries into these areas.[70] This frustrated their abilities to assess more systemic failings within the communications data processes.

Further, when errors were detected with authorisations, the powers of the IOCC were inadequate. Despite a number of errors consistently occurring in the authorisation process, until 2013, the IOCC had yet to direct a public authority to provide information to an individual who has been adversely affected by any wilful or reckless exercise of, or failure to, exercise its powers under the Act.[71] Furthermore, the Commissioner could not inform those individuals who have not been subject to a 'serious error' i.e. one which causes significant prejudice or harm to the person concerned.[72] In addition, the serious errors of which people could be informed were only those committed by public authorities; leaving a gap in protections for those errors committed by CSPs (approx. 13% of serious errors).[73] Such limitations called into question the protection such error reporting provided individuals.

In addition to a lack of independence and limited powers, the ability of the IOCC to effectively oversee the provisions of the investigatory powers instruments was further diminished by the fragmented nature of the oversight regime and the use of a single Commissioner structure. Prior to the introduction of the 2016 Act, oversight of the use of surveillance powers by public authorities was spread amongst the Surveillance Commissioner, the Intelligence Services Commissioner, and the Interception of Communications Commissioner. Such a regime led to a highly fragmented and

[70] Burnton n(48) para 5.6; this has been included in the remit of the IPC under the Investigatory Powers Act 2016.
[71] Anthony May, *Annual Report of the Interception of Communications Commissioner* (HC1184, 2013) 36.
[72] Burnton n(48) para 5.18.
[73] *Ibid.*

inefficient system. Critiques of the regime consistently called for the creation of a single body, placed on statutory footing, to counter the oversight gaps and remove overlaps. Throughout the legislative process which culminated in the Investigatory Powers Act, various Committees and interested parties offered recommendations for ways to improve the oversight regime.

Notably, David Anderson, then Independent Reviewer of Terrorism Legislation, drafted a comprehensive report in which he proposed a shift in the structure and power of the supervisory agencies to better ensure meaningful oversight. Anderson recommended that instead of the fragmented regime under previous instruments, wherein separate bodies were responsible for different areas of the same act (i.e. IOCC for interferences and communications data; Intelligence and Security Committee for oversight of intelligence agencies; etc.), these bodies should be merged into a single responsible agency. This agency would not be a single Commissioner but rather a Commission which would be 'a well-resourced and outward-facing regulator of all those involved in the exercise of surveillance powers and of the security and intelligence agencies more generally'.[74] This Independent Surveillance and Intelligence Commission (ISIC) would take on the existing powers of audit and inspection, but also take on the warrant and authorisation issuing powers, thereby removing those powers from the Home Secretary and vesting them in an independent judicial body.[75] Anderson's recommendations were endorsed by members of the oversight bodies, the Joint Committee on the Investigatory Powers Bill, and various NGOs; however, despite this support, they were not wholly incorporated in to the IPA.

[74] Anderson n(45) 14.94.
[75] Anderson n(45) 14.95.

V. The role of the Investigatory Powers Commissioner (IPC) in overseeing communications data

Rather than the Commission model advocated by Anderson and others, the Investigatory Powers Act amended the Commissioner system by creating the office of the Investigatory Powers Commissioner. The relevant aim of the Commissioner is to provide effective oversight of the communications data powers of public authorities. It is necessary to examine how the Commissioner achieves this aim in order to determine if it can satisfy requirements of independent oversight of communications data powers.

a. Functions and Powers of the Investigatory Powers Commissioner

The structure of the IPC differs from the IOCC by requiring not only a sole Commissioner but supplementing him with thirteen Judicial Commissioners who have oversight remit. Both the Commissioner and his Judicial Commissioners are appointed;[76] these officeholders may not be appointed unless they hold or have held prior judicial appointment of at least the level of high court judge.[77] In practice the Judicial Commissioners are composed of current and recently retired High Court, Court of Appeal, and Supreme Court Judges. The current Commissioner is Lord Justice Sir Adrian Fulford, a serving Lord Justice of Appeal and former Senior Presiding Judge for England and Wales.[78] The independence of the Commissioners is guaranteed by the limited circumstances in which they can be removed from office; i.e. only with the consent of both Houses of Parliament, unless extraordinary circumstances apply.[79] To

[76] Adrian Fulford, 'Investigatory Powers Commissioner's Office Press Release on the Appointment of Judicial Commissioners' (18 Oct 2017) < https://www.judiciary.gov.uk/wp-content/uploads/2017/10/jc-announcement-13-new-commissioners-oct2017.pdf> accessed 19 Oct 2017.
[77] Explanatory Notes to the Investigatory Powers Act 2016 para 633.
[78]IPCO, 'Who we are', (*Investigatory Powers Commissioner's Office* 2018) < https://www.ipco.org.uk/default.aspx?mid=14.12> accessed 15 Jan 2018.
[79] Investigatory Powers Act 2016 s 228(4)-(5). Extraordinary circumstances include being given a prison sentence or being disqualified from being a company director.

satisfy his functions, the Commissioner is provided with a staff of around 70 people – roughly twice the size of the three predecessor organisations whose functions the IPC has undertaken. This staff, as well as other facilities, accommodation, and resources, are provided to the IPC by the Home Secretary.[80] The Secretary will provide the resources they consider necessary, but the IPC may request additional resources be afforded to them in their Annual Report.[81]

The Annual Report is one of the primary duties of the IPC and provisions concerning this largely replicate those that existed under the IOCC regime. This report must be laid before the Prime Minister and will provide an account of the work done by the IPC. In addition, the Prime Minister may require the IPC to provide additional reports. Similarly, the IPC can initiate its own reports on any matter that the Commissioner has oversight of and provide recommendations that he believes appropriate.[82] The ability of a body to initiate investigations such as this on their own is recognised as a crucial element of oversight powers.[83] Once a report is submitted to the Prime Minister, she has a duty to lay that report before Parliament. However, the reports may be redacted in order to preclude disclosure of any information that is believed to damage national security or operational effectiveness.[84]

The IPC and other Judicial Commissioners have discretion with regard to how they fulfil their functions, whether through audits, inspections, and investigations.[85] However, in doing so the IPC must ensure that their activities do not impede the ability of law enforcement and security and intelligence agencies to perform their statutory functions.

[80] IPA s 238.
[81] Explanatory Notes to the IPA para 658.
[82] IPA s 234
[83] European Union Agency for Fundamental Rights n(23) 78.
[84]Explanatory Notes to the IPA para 650.
[85] IPA s 229.

The IPC has a positive duty not to act in a way that would, for example, prejudice national security or impede the effectiveness of operations.[86] This places a constraint on the oversight capabilities of the IPC and runs contrary to the core of judicial scrutiny in ensuring that these powers are exercised in accordance with the principles of the rule of law. Notably, in examining the issue of data surveillance, the Fundamental Rights Agency has stated that an important factor in assessing the effectiveness of an oversight system is whether the body has the power to quash authorisations, stop surveillance, and require the rectification or erasure of collected data.[87] Whilst the IPC has powers with regard to quashing retention notices and stopping surveillance measures already undertaken, their abilities with regard to the rectification and erasure of data are limited. It is necessary to examine the extent to which the powers of the IPC in fact enable effective judicial oversight and whether they are subject to any limitations that would frustrate their role in ensuring the collection and processing of communications data accords with the rule of law.

b. Criticisms of the Investigatory Powers Commissioner

Upon undertaking the role of Investigatory Powers Commissioner, Sir Adrian Fulford promoted the necessity of the independence of the office. 'Independence is at the heart of the new organisation; IPCO is an Arm's Length Body of the Home Office but retains the authority to perform its statutory duties'.[88] Despite this pledge for independence and the improvement in statutory independence requirements under the IPA, many of the issues inherent with the previous oversight structure remain. Namely, the Home Secretary still

[86] IPA s 229(8).
[87] European Union Agency for Fundamental Rights n(23) 78.
[88] Adrian Fulford, 'Investigatory Powers Commissioner's Office Letter response to Privacy International, Liberty, Big Brother Watch, and the Open Rights Group' (13 Oct 2017) < https://ipco.org.uk/docs/2017%2010%2013%20IP%20Commissioner%20response%20to%20Privacy%20International%20et%20al.pdf> accessed 19 Oct 2017.

remains responsible for the provision of funding, facilities, and staffing as they deem necessary. This means that there still exists a financial dependency which is of significant concern for its independence. The resources allocated will be those deemed necessary by the government agency whom the IPCO is ultimately responsible for overseeing. Indeed, this is particularly salient as the IPCO now serves as a 'double lock' on the warrant process. All retention notices issued under IPA must not only be signed off by the Home Secretary, but also approved by the IPCO or one of his Judicial Commissioners.[89] The availability of resources which the IPCO may devote to the scrutiny of each notice will be constrained by budgetary and staffing considerations. In addition, the allocation of the annual budget will be put forth by the Home Office. Any approvals for additional funds would have to be included in the Home Office allocation. There is a dependency between the IPCO and the Home Office which undermines the independence, whether real or perceived, of the office.

More significant criticisms for the IPCO can be offered in regard to the limited powers it has concerning communications data access. These criticisms concern authorisations for access to communications data, error reporting provisions, and the lack of appropriate mechanisms for redress for individuals under the IPC scheme.

First, concerns remain over the inability of the oversight regime under the IPA to offer independent judicial scrutiny for applications prior to the disclosure of the relevant information. This is in direct contrast to established precedent. In the case of *Digital Rights Ireland*, for example, the CJEU held that Directive 2006/24/EC failed because,

> Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or an independent

[89] IPA Part 8.

> administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary....Nor does it lay down a specific obligation on Member States designed to establish such limits.[90]

The IPA does not meet these criteria; there is no requirement for prior independent judicial authorisation to access communications data. The IPC is only able to scrutinise the retention notices which place an obligation on CSPs to retain data; they have no remit to scrutinise subsequent applications for access by law enforcement. Prior judicial scrutiny is crucial to ensure that the exercise of the powers comports with the rule of law and guarantees that those in power can be held accountable for their actions.

It is important to acknowledge that the Courts have held that the requirement for effective oversight can be met absent formal judicial control provided that the control is exercised by an official qualified for judicial office.[91] The fact that oversight is not undertaken by a judicial body would not appear, in itself, to satisfy a finding that the oversight regime is inadequate. Qualifications aside, there is a question of the adequacy of the process as a mechanism that meets the standards of independent oversight. The office has no role in *ex ante* authorisations to access communications data. The IPCO will only be engaged in approving notices to retain data and authorising access for those 'privileged professions' such as journalists, lawyers, and MPs. Absent that, the IPC does not provide judicial control over the access process. While the European Courts have held that such authorisation is not mandatory *per se* provided that there is extensive *post*

[90] *Digital Rights Ireland* n(10) para 62.
[91] This was established in *Klass & Ors v Germany* App no 5029/71 (ECtHR, 6 Sept 1978) para 56 and *Szabo* n(9) para 85.

factum review to counterbalance the shortcomings,[92] the Court did question any process which failed to do so in a blanket manner.[93]

Even with a review *ex post,* the ability of the IPC in being able to provide such scrutiny effectively is questionable. The sheer number of communications data authorisations mean that it is impossible for the Judicial Commissioners to review all authorisations. Review will necessarily only happen by sampling, which can limit the perceived effectiveness of these provisions. In addition, as Judith Rauhofer notes, 'Retrospective review is likely to be less rigorous than prior scrutiny and it may well be easier to satisfy the requirements of necessity and proportionality when armed with the incriminating results of the surveillance'.[94] Further, errors are unlikely to be found by the Judicial Commissioners unless they are specifically reported to them by the relevant CSP or public authority. As a result, instead of performing an independent and open check, the primary oversight mechanism relies on self-reporting. This is insufficient to mitigate privacy intrusions and offers only a veneer of oversight.

Where serious errors are detected, the powers of the IPC remain constricted in much the same manner as the IOCC. Under s 231 of the IPA, the IPC is entitled to inform individuals of serious relevant errors in the use of investigatory powers which relate to them. Here a relevant error is 'an error made by a public authority in complying with any requirement over which the Investigatory Powers Commissioner has oversight'.[95] This provision remains a power that *may* be exercised rather than a mandatory requirement. Further, the right to inform an individual is limited to those instances where it is both in

[92] *Kennedy* n(13) para 167 and *Szabo* n(9) para 77.
[93] *Digital Rights Ireland* n(10).
[94] Judith Rauhofer, 'Privacy and Surveillance: Legal and Socioeconomic Aspects of State Intrusion into Electronic Communications' in Edwards and Waelde (eds), *Law and the Internet* (Hart Publishing 2009) 561.
[95] Explanatory Notes to the IPA para 643.

the public interest to inform the individual and significant prejudice or harm to the person concerned has resulted.[96] A similar argument was put forth in *S & Marper v United Kingdom* and was held to be an insufficient justification for retention. In that case, the Government argued that 'retention could not be considered as having any direct or significant effect on the applicants unless matches in the database implicated them in the commission of offences on a future occasion'.[97] This arguably prioritises the law enforcement objectives over human rights concerns as it looks to subsequent rather than current harms and violations.

It is for the IPC to undertake an examination of the error and balance the seriousness against the public interest in non-disclosure. This is a discretionary power; there are no binding or determinative requirements for conduct that will amount to 'serious'. The final report of the IOCC before its powers were undertaken by the IPC noted that the Commissioner would only notify the individual if 'significant prejudice or harm (such as being arrested)' occurred.[98] It is questionable whether lower interferences with individual rights, such as searches of homes or devices, or visits by the police which could potentially have similar negative effects on individuals would meet the Commissioner's definition of 'significant prejudice or harm'. This provision is therefore open to criticism. In determining seriousness, the emphasis appears to be on the consequences of the error rather than the seriousness of the conduct.[99] Judging errors in this way thereby focuses on individual harms rather than more systemic issues that might arise from the conduct of public authorities. Finally, the requirement that there be 'significant prejudice or harm' sets the threshold artificially high. This can prevent

[96] Explanatory Notes to the IPA para 644.
[97] *S and Marper* n(14) para 121.
[98] Burnton n(48) 19.
[99] Burnton n(48) para 5.18.

individuals from being able to seek adequate remedies for undue breaches of their privacy resulting from communications data processes.

The ability of individuals who have been negatively impacted by the communications data powers to seek an effective remedy is crucial to ensuring that the interference occasioned by the actions of public authorities is justified. In order to effectively exercise their right to remedy, individuals need to be notified of when their data has been used. It was held in the case of *Tele2 and Watson* that 'the competent national authorities to whom access to the retained data has been granted must notify the persons affected...as soon as that notification is no longer likely to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable to persons affected to exercise, inter alia, their right to a legal remedy'.[100] This established case law is supported by bodies such as the UN[101] and the Venice Commission[102] who reiterate the necessity of notification for individuals who have been subjected to actions by public authorities, including communications data surveillance. The IPC should be entitled to inform individuals who have been subject to this surveillance, once it no longer poses a risk to the aims of the retention and access. Yet there remains no explicit

[100] *Joined Cases C-203/15 Tele2 v Post-och telestyrelsen & C-698/15 Watson & Ors v Secretary of State for the Home Department* (2016) ECLI 970 para 121; Case C-362/14 *Max Schrems v Data Protection* Commissioner (2015) ECLI 650 para 95; *Weber and Saravia* n(10) para 135; C-553/07 *College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer* [2009] ECLI 293 para 52; *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 Dec 2015) para 287; and *Szabo* n(9) para 86. However, this precedent seems to directly conflict with the ruling in *Klass* n(83) para58 where it was held that 'In the Court's view, in so far as the "interference" resulting from the contested legislation is in principle justified under Article 8 para 2, the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the "interference".'

[101] See Frank La Rue, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (UN 2013) A/HRD/23/40 which found that: 'individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the state' para 82.

[102] 'Individuals who allege wrongdoing by the State in other fields routinely have a right of action for damages before the courts. The effectiveness of this right depends, however, on the knowledge of the individual of the alleged wrongful act, and proof to the satisfaction of the courts.'

requirement of notification in the IPA.[103] As a result, individuals are severely limited in their abilities to seek remedies. 'Effectiveness [of remedies] is therefore undermined by the absence of a requirement to notify the subject of an interception at any point, or an adequate possibility to request and obtain information about interceptions from the authorities'.[104] As the powers conferred on the IPC do not enable notification and thereby promote access to remedies, it is necessary to determine what rights the individual may have to challenge the retention or access of their data by public authorities. Under the investigatory powers provisions, the only right to redress that an individual has is offered by the Investigatory Powers Tribunal.

VI. The role of the Investigatory Powers Tribunal (IPT): judicial oversight for communications data?

As the principal mechanism for challenges to powers of retention and access, it is necessary to examine the scope and capabilities of the Investigatory Powers Tribunal in adjudicating human rights claims which arise from the use of investigatory powers instruments. The IPT itself has been the court of record for complaints concerning interception of communications and related data since these powers were first put on a statutory footing. In its earliest iteration under the Interception of Communications Act 1985, the Tribunal was entitled to investigate whether there were relevant warrants or certificates issued for intercepted information, and, if so, whether there were any contraventions of the provisions of the Act.[105] If the Tribunal found that there had indeed been a contravention, notice was to be provided to the applicant and Prime Minister, and,

[103] European Union Agency for Fundamental Rights n(23) 126; The report notes that out of the 5 Member States that have detailed legislation on general surveillance of communications, only Germany and Sweden stipulate a notification requirement in cases of general surveillance of communication.

[104] *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 Dec 2015) para 298.

[105] Interception of Communications Act 1985 s 7.

where applicable, the relevant warrant would be quashed, intercepted material destroyed, and compensation ordered.[106] In essence, as the IPT saw it, their role was 'largely retrospective, to check that warrants had not been issued in contravention of the Act and that appropriate procedures were followed'.[107]

Subsequently, the powers of the Tribunal originally granted under the ICA 1985 were subsumed into RIPA. RIPA provided the IPT with the power to decide complaints and claims under the Human Rights Act 1998 (HRA) of allegations of unlawful intrusions by public bodies, the police, and local authorities, including those complaints which relate to the acquisition of communications data. Under ss 65-69 RIPA, the IPT is entitled to consider, and if necessary investigate, complaints made by members of the public for unlawful access or actions which do not meet the requirements of necessity and proportionality.[108] By providing a mechanism for the investigation of complaints and HRA claims, RIPA sought to meet the requirements for a right to remedy as established under Article 13 of the ECHR. This Article requires that 'everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity'.[109] The validity of the IPT in discharging this function was accepted in the case of *Kennedy v United Kingdom.*[110] The RIPA provisions concerning the IPT have now been largely incorporated into the IPA, with a few notable developments as regards powers and functions.

[106] *Liberty* n(8) para 29.
[107] Bingham n(44).
[108] Investigatory Powers Tribunal, *Report of the Investigatory Powers Tribunal*, (2016) http://ipt-uk.com/docs/IPT%20Report%202011%20-%202015.pdf para 1.4
[109] European Convention on Human Rights Article 13 given domestic effect under the Human Rights Act 1998.
[110] *Kennedy* n(13).

A. Functions and Powers of the Investigatory Powers Tribunal

Before turning to the relevant criticisms of the IPT, it is first worth noting the scope of its powers and its primary functions as regards the collection and processing of communications data. The IPT is fundamentally different from traditional courts. It is not a part of Her Majesty's Courts and Tribunal Service; nor is it a *senior* court which can make a declaration of incompatibility with the ECHR pursuant to the HRA s 4.[111] It is classed as a Tribunal non-departmental public body of the Home Office.[112] The Tribunal does not occupy a primarily adjudicative role; rather its principal function is investigatory. It can follow through on questions which arise by ordering investigations with which the public authorities are required to cooperate.[113] The investigatory functions of the IPT sit uneasily with the traditional judicial structure and application of the principles of judicial review. In addition, the Tribunal's powers are reactive; they are derived from receiving a claim or a complaint.[114] Once a complaint is received and investigated, the Tribunal uses the principles of judicial review to determine any potential remedy.

In fulfilling their investigatory role, the IPT has several unique features. The Tribunal is entitled to demand, receive, and consider evidence even where such evidence would be inadmissible in an ordinary court.[115] The demand for this evidence must be complied with by public authorities.[116] It is for the public authorities to provide the requested information to the IPT for the purposes of their investigation. However, this will be

[111] Anderson n(45) 6.111(d).
[112] The other bodies which are classified in this manner are the Office of Surveillance Commissioners and the Police Discipline Appeals Tribunal.
[113] Investigatory Powers Tribunal Rules 2000, SI 2000/2665, 2.1.
[114] Investigatory Power Tribunal, *Report of the Investigatory Powers Tribunal*, (2016) <http://ipt-uk.com/docs/IPT%20Report%202011%20-%202015.pdf> para 1.6.
[115] *Ibid* para 2.2.
[116] RIPA s 68(6).

based on trust. There is no process for the IPT themselves to audit any records or gain access to the records themselves; the only evidence which is provided is that given by those under investigation. This further contributes to criticisms of the efficacy of the IPT as an effective oversight mechanism. In theory, the investigatory powers of the IPT in demanding evidence have a broad scope: individuals can be ordered to appear to give evidence; organisations' files can be requested; and the Commissioners, such as the Judicial Commissioners discussed above, must provide any documents, information, or assistance to the Tribunal which is requested.[117]

The Tribunal may place limits on the disclosure of information to the parties concerned. Such limitations on disclosure in the interest of national security or for the investigation of crime have received judicial approval and have been held to not directly interfere with human rights standards.[118] In order to ensure confidentiality, the IPT is entitled to provide anonymity to witnesses, applicants, and other interveners in the case. This is allegedly necessary in many instances to ensure the protection of national security and ensure that sensitive information is not disclosed. The anonymity provisions are coupled with similar powers to hold closed hearings wherein not all the relevant parties are entitled to attend and decline to hold oral hearings.[119] Where oral hearings are held, there is no requirement that the respondent or complainant be entitled to make representations, give evidence, call witnesses, or even attend.[120] Further, there is no automatic right to open hearings under the IPT Rules.

[117] IPA s 232.
[118] *Kennedy* n(13) para 187.
[119] IPT Rules n(113) 9(2).
[120] *Ibid* 10(1)

Yet, at their discretion, the IPT may hold a public hearing. This was done for the first time in January of 2003.[121] There has been a rise in the number of public hearings since then, however, the more common practice remains closed hearings. Indeed, hearings in the traditional adversarial sense are rarely held at all. Rather, the IPT will meet to review the documents and then provide notification of the outcome.[122] In addition to the lack of open hearings, the sensitive nature of the material relating to many of the complaints further means that 'the complainant may not be aware of what [the Tribunal] has seen and will not be entitled to hear or see it'.[123] This represents a significant information disparity between the complainant and the public authority. However, this has been held not to inhibit the complainants' right to a fair trial as established in *Kennedy v UK*. 'In reaching this conclusion, the Court emphasises the breadth of access to the IPT enjoyed by those complaining about interception within the United Kingdom and the absence of any evidential burden to be overcome in order to lodge an application with the IPT'.[124]

Key to the ECtHR decision was the breadth of access provided to the IPT by the authorities under investigation. The ability to investigate this material and the ability of the complainant to access the court were seen as sufficient to meet the necessary standards for a fair trial under Article 6, particularly given the secret nature of the information allegedly intercepted by the authorities.[125] In this case the ECtHR afforded a wide margin of appreciation to the State in the use of its investigatory powers. However, the Court in its ruling paid particular attention to the nature of the material at issue and

[121] *Kennedy v Security Services, GCHQ and the Metropolitan Police Service* and *British-Irish Rights Watch & Ors* IPT/01/62 and IPT/01/77 (IPT 23 Jan 2003).
[122] Ian Cobain and Lelia Haddou, '"Independent" court scrutinising MI5 is located inside Home Office' (*The Guardian* 5 Mar 2014) < https://www.theguardian.com/politics/2014/mar/05/independence-ipt-court-mi5-mi6-home-office-secrecy-clegg-miliband> accessed 11 Nov 2017.
[123] IPT n(114).
[124] *Kennedy* n(13) para 190.
[125] *Kennedy* n(13) para 169.

the need for secrecy surrounding that type of information; if *Kennedy* was argued with regard to communications data it is arguable that these issues would need to be re-examined, paying particular attention to the blanket nature of the communications data powers and the lack of any statutory limitations which require its use only in instances of 'serious crime'.

Once a complaint has been investigated, the Tribunal will make a determination which can lead to one of seven possible outcomes. The first of which is that no determination can be made in favour of the complainant. Under this outcome, the Tribunal will either be satisfied that no wrongful conduct has occurred or that the conduct was not in contravention with the Act and was proportionate.[126] There is no requirement, if no determination has been made, to inform the complainant as to which of these reasons apply. To provide this information to the individual has been held to frustrate the purposes of the powers granted under the investigatory regime. A ruling of no determination has been held to be sufficient for the principles of judicial remedy.[127] The second potential outcome which can arise is that the complaint is out of jurisdiction, meaning the IPT has no power to investigate the complaint.[128] The third possible outcome is that the complaint was lodged after the relevant time and the time limit should not be extended.[129] Fourth, the complaint might be ruled frivolous or vexatious if it lacks foundation or is repeatedly taken.[130] Fifth, the complaint might be dismissed due to procedural reasons. The sixth outcome will result in no determination where the complainant has since withdrawn the complaint. The final potential outcome is that the Tribunal finds in favour of the complainant. In this case it is open to the Tribunal to

[126] IPT n(114) para 1.6.
[127] *Kennedy* n(13) para 189.
[128] IPT Rules n(113) 13(3)(c).
[129]IPT Rules n(113) 13(3)(b).
[130] IPT Rules n(113) 13(3)(a).

issue an order quashing or cancelling the relevant warrant or authorisation, order the destruction of records or information which have been obtained, and/or order compensation be paid.[131] There is little guidance offered by the IPT on what will result in a finding in favour of the complainant. Statements made by the President of the IPT indicate that the Tribunal evaluates the requirements of necessity and proportionality, having particular regard to the balance of public interest versus the individual harm suffered. The low success rate of claimants to this Tribunal give rise to the inference that the margin of appreciation here is heavily weighted toward the State.

Where a determination is made in favour of the complainant, the complainant is then entitled to a summary of that determination, including any findings of fact.[132] However, in providing this information, the duty to give reasons and information concerning the findings will vary according to the nature of the decision and the circumstances of the case. If the Tribunal declines to give reasons on the basis that it will jeopardise national and/or law enforcement interest, the competent national authority must prove that the giving of reasons is against the public interest. If these interests do stand in the way, precedent dictates that there must be an appropriate balance between these interests and the requirements of the right to effective judicial protection, where any interference of that right is limited to what is strictly necessary.[133]

Whilst this indicates that the IPT operates as a judicial check on the abuse of powers in the field of communications data, public confidence in the Tribunal as an effective oversight body is diminished by the typical outcomes of these cases. From 2000-2013, the IPT heard 1,673 complaints, out of which only 10 were upheld, 5 of which related to

[131] As regards the latter the Tribunal has only awarded costs on one occasion in the case of *Chatwani & Ors v NCA* [2015] UKIPTrib 15_84_88-CH.
[132] IPT n(113) Art 15(2).
[133] C-300/11 *ZZ v Secretary of State for the Home Department* [2013] ECLI 363 paras 60-64.

the same family.[134] Whilst not necessarily indicative that the IPT serves as a mere façade of judicial scrutiny for the fundamental rights interfered with under the investigatory powers mechanisms, it does raise concerns. The list of public authorities entitled to use powers under IPA is expansive; the low success rate of complainants indicates that these authorities consistently use these powers in accordance with the precise letter of the law, to the extent that 95.5% of applications to use these powers precisely comply with the letter of the law.[135] Such a low rate of success for complaints creates the public perception that the Tribunal is not a truly effective mechanism for individuals to get a determination regarding their complaints. As perhaps best summarised in the JUSTICE report 'Freedom from Suspicion': '[It] beggars belief that public bodies and government departments that struggle to produce defensible decisions in the field of planning, pension credits, and incapacity benefits are somehow incapable of making mistakes when it comes to surveillance'.[136]

Furthermore, the lack of transparency regarding successful decisions raises concerns as to the accountability of the IPT. The IPT has published two annual reports which are publicly accessible, one covering 2011-2015 and one for 2016.[137] The IPT only sat in public for the first time in 2003 and held that their decisions could be made publicly available provided Neither Confirm nor Deny (NCND) was not violated and no risk to national security or the public interest was present.[138] It was not until 2013 that the President of the Tribunal gave any sort of public interview.[139] Whilst recent

[134] Anderson n(45) 6.106.
[135] JUSTICE n(68) 139.
[136] JUSTICE n(68) 139.
[137] Investigatory Powers Tribunal, *Annual Reports 2011-2015* (2016) < http://ipt-uk.com/docs/IPT%20Report%202011%20-%202015.pdf>.
[138] *Kennedy* v *Security Services* n(121).
[139] Law in Action, Interview with Justice Burnton , President of the Investigatory Powers Tribunal, BBC Radio 4 (7 Nov 2013).

developments of the IPT with regard to open hearings and positive obligations to give reasons, provided security or public interest concerns are not raised, are important developments, the functions and powers of the IPT still lack transparency. The limitations of the IPT will now be analysed in greater detail.

c. Criticisms of the Investigatory Powers Tribunal

Low success rates do not automatically equate with an inability to garner a legitimate remedy in line with relevant human rights standards. In this regard it is necessary to examine further criticisms which are raised about the IPT to appropriately assess whether it is an acceptable safeguard for individuals' rights concerning communications data. Several concerns are raised when discussing the legitimacy of the IPT: independence and the judicial role of the Tribunal; the transparency of the Tribunal process; the amenability of decisions of the Tribunal to further review or appeal; and the ability of individuals to secure adequate and effective relief. Each of these criticisms will be addressed to determine the effectiveness of the IPT as an oversight mechanism.

As noted above, the Tribunal is distinct from traditional English courts as it possesses an investigative function. It is difficult to equate these functions with the independent judicial functions of a court. Rather, as noted in the JUSTICE report 'Freedom from Suspicion', 'the Tribunal represents an attempt to combine the investigative functions of an Ombudsman with the judicial functions of a court'.[140] Such a distinction was made when the tribunal was first proposed under the ICA 1985. Then Home Secretary, Mr. Leon Brittan, in describing the tribunal noted that the 'arrangements are, in substance, the same as those which apply to the Ombudsman and they secure the tribunal's complete

[140] JUSTICE n(68) 135.

independence'.[141] The arrangements referred to included that the tribunal consist of senior lawyers, appointed by the Crown, and may only be removed by both Houses of Parliament. The current iteration of the IPT has the same structure as its predecessor. Appointments are ultimately undertaken by the Prime Minister who may appoint either 'judicial members' who are a serving member of the senior judiciary, or 'non-judicial members' who may be senior members of the legal profession.[142]

Rather than being overseen by Her Majesty's Courts and Tribunal Service who is responsible for promoting an independent judiciary, the IPT is overseen and sponsored by the Home Office. As the IPT remains a non-departmental public body of the Home Office it is argued that they are not manifestly independent of those whose decisions they are reviewing. In the same manner as the IPC, budgetary considerations and funding decisions must also be approved by the sponsoring department and their offices are located within the Home Office.[143] Whether perceived or in practice, such an arrangement raises concerns over the true independence of the IPT, particularly as it is the only body with domestic jurisdiction over the investigatory powers instruments. This means that the body ultimately responsible for reviewing the legality of interferences with individuals' data which impact on individuals rights is closely linked to the Home Office who issues the warrants and retention notices that enable them to do so.

In addition to the question of independence, the effectiveness of the IPT as a means of redress for complainants who have suffered a violation under IPA is further frustrated by the opaque procedures of the Tribunal. Lack of disclosure and transparency creates

[141] HC Debates col 162, 12 March 1985.
[142] Investigatory Powers Tribunal, 'Appointment Process' (*Investigatory Powers Tribunal*, 5 Jul 2016) <*https*://www.ipt-uk.com/content.asp?id=21>.
[143] This is the Office location known as of 2014. See: Cobain n(122).

barriers for access to justice and has a negative impact on complainants' abilities to challenge unlawful activities. Yet, this opacity lies at the heart of the powers of the IPT. This is in direct contradiction to the traditional judicial process which occurs in an open court and enables both sides to engage in an adversarial process. In introducing the Tribunal in 1985, Leon Brittan, justifying the lack of information provided to claimants, stated that 'it would clearly, however, be ridiculous for somebody to be able to discover whether an interception had been directed against him by applying to the tribunal'.[144]

The current Tribunal rules provide that,

> The Tribunal should carry out their functions in such a way as to secure that information is not disclosed to an extent or in a manner that is contrary to the public interest or prejudicial to the national security, the prevention or detection of 'serious crime', the economic wellbeing of the United Kingdom, or the continued discharge of the functions of any of the intelligence services.[145]

Prevention of disclosure may be necessary in limited instances but as a standard practice of the sole body with jurisdiction to rule over human rights concerns wrought by the IPA it represents a substantial impediment to justice. The materials obtained by the IPT as part of their investigatory role are often the primary information used to decide a case. Since that information is not required to be provided to the complainants, the Tribunal is typically limited to confirming that an investigation is still ongoing.[146] The complainant has no right to challenge or access the information that forms the foundation of a decision relevant to him.

[144] HC Debates col 163 March 1985.
[145] IPT Rules n(113) 6.
[146] IPT n(114) para 2.17.

Furthermore, while the IPT can demand that the relevant bodies disclose information pertinent to their investigation to the Tribunal should they consider that the information be made available to the claimants, they cannot make a demand that the authorities disclose the information to the other parties; they may only request that they do so.[147] This is a weak mechanism for ensuring informational parity. As Lord Kerr stated in his dissent in the case of *Home Office v Tariq* when discussing closed material procedures, 'withholding of information from a claimant which is then deployed to defeat his claim is, in my opinion, a breach of his fundamental common law right to a fair trial'.[148] The European Courts have echoed similar concerns, 'The fundamental right to an effective legal remedy would be infringed if a judicial decision were founded on facts and documents which the parties themselves, or one of them, have not had an opportunity to examine and on which they have therefore been unable to state their views'.[149] Despite this, certain exceptional cases have entitled national authorities to limit the provision of information to complainants. This was the case in *Kennedy v United Kingdom* which challenged the secrecy of the IPT's disclosure practices. In that instance, the procedures were validated; despite the limited access, the right to a fair trial under Article 6 was not infringed. However, it is notable that the proceedings in *Kennedy* were validated because the prohibition on disclosure was not absolute; a policy of blanket refusal would likely fall foul of these proceedings.

However, whilst a policy of blanket refusal to provide information to claimants is not enshrined in the IPT rules, the accepted practice of NCND in effect guarantees that claimants will not be provided with the necessary information to validate their claims.

[147] JUSTICE, *To "Neither Confirm Nor Deny": Assessing the Response and its Impact on Access to Justice* (2017) 14.
[148] *Home Office v Tariq* [2011] UKSC 35 para 108.
[149] Case C-89/08 *European Commission v Ireland & Ors* [2009] ECLI para 52; *ZZ* n(133) para 56.

The position of the IPT is to accept NCND where it is deemed to be lawful and serves a legitimate purpose. The IPT for its part will neither confirm nor deny whether a warrant or authorisation has been issued against an individual unless that conduct is subsequently found to be unlawful.[150] As noted by Sir Justice Burnton in a BBC interview, the role of the IPT is solely to make a determination as to whether there had been a breach of the law.[151]

The willingness of the IPT to accept allegations that material must be subject to NCND must be criticised. In its 2011 Report, JUSTICE noted that 'the IPT have generally been too accepting of public authorities decisions to use an NCND response'.[152] In accepting the request of a public authority to NCND the existence of materials that give rise to an interference with individuals' rights, there is a threat to open justice and procedural fairness. Individuals cannot challenge that information to which they have no access. The tendency to invoke NCND as an automatic or routine procedure by public authorities in this area can cause further issues where the information is eventually disclosed. This occurred in the IPT in the *Belhadj* case, where late disclosures were made which impacted on *Liberty/Privacy (No 1)* and were later considered in *Liberty/Privacy (No 2).*[153] Late disclosures following an initial NCND suggested that an appropriate analysis of the true need for NCND was not adequately evaluated by the IPT. Furthermore, as Judith Rauhofer notes, if communications data is less intrusive, as frequently argued by the Government, 'then surely the body responsible for overseeing such use can afford to

[150] IPT n(114) 2.2.
[151] Law in Action n(139); This was the first interview given by any member of the IPT and it did not occur until 2013, 13 years after the Tribunal came in to effect
[152] JUSTICE n(68).
[153] JUSTICE, *To "Neither Confirm Nor Deny'* n(139) 14; See also: *Privacy International v Secretary of State for Foreign and Commonwealth Affairs & Ors* [2016] UKIPTrib 15_110CH; *Belhadj & Ors v Security Service & Ors* [2015] UKIPTrib 13_132-H.

be more open about the failures to meet legislative requirements without jeopardising ongoing inquiries or the position of those requesting information'.[154]

In addition to the limited provision of information to complainants, a further impediment to individuals' access to justice concerns the requirements that the IPT sit in private and the provision that principal parties can be excluded from attending these proceedings. There is no requirement for the IPT to hold oral hearings. Even where such hearings are held, there is no requirement that the Tribunal disclose to the complainant that these hearings have occurred.[155] However, the IPT does have discretion to grant oral hearings and even permit open hearings should they believe it is necessary to do so. The Tribunal can similarly make public their transcripts or reasoning if they so choose.[156] Whilst this discretionary power exists, open proceedings under the IPT remain the exception rather than the rule. Once again *Kennedy* has been offered as substantive support for the provisions against open procedures under the IPT.[157] However, new challenges to the regime are going through the Courts which might result in a different outcome. Notably the case of *Big Brother Watch and Ors v United Kingdom* calls into questions the compatibility of the IPT's procedures with the provisions of Article 6.[158] Once decided this case may potentially provide further precedent for the role of the IPT.

The IPT does attempt to balance the limitations of these closed procedures by conducting cases based on 'assumed' facts. Under this provision, where points of law arise the Tribunal, without making any finding on the substance of the complaint, 'may be

[154] Judith Rauhofer, 'The Retention of Communications Data in Europe and the UK' in Edwards and Waelde (eds) *Law and the Internet* (Hart Publishing 2009) 593.
[155] IPT Rules n(113) 6(2)(a).
[156] *Kennedy v Security Service* n(121).
[157] *Kennedy* n(13) para 161.
[158] *Big Brother Watch and Others v. the United Kingdom* App no 58170/13; *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom* App no 62322/14; and *10 Human Rights Organisations and Others v. the United Kingdom* App no 24960/15 [cases pending before the ECtHR].

prepared to assume for the sake of argument that the facts asserted by the claimant are true; and then, acting upon that assumption, decide whether they would constitute lawful or unlawful conduct'.[159] This allows the Tribunal to reach a conclusion based on those assumed facts. Subsequent to this, if the conduct based on assumed facts is judged to be unlawful, the IPT will then consider the issue in closed session.[160] Following consideration of that issue, the IPT may make a determination in line with the outcomes discussed in the preceding section. Yet despite this provision concerning assumed facts, the closed procedures and lack of disclosure put the claimant at an informational disadvantage in arguing his case. Furthermore, the use of assumed facts has been used by the IPT to preserve the public authorities' use of NCND which creates additional obstacles for complainants.

This has led to a situation where the odds are stacked against the complainant. The principles of closed procedures are all the more problematic when noting that the procedures of the IPT are not open to judicial review. Judicial review ensures that adjudicative bodies may be held to account and that the decisions made therein satisfy the requirements of legality. Judicial review is procedural in nature; it is not for re-examining the merits of a case nor substituting a different judgment for the decision of the IPT. The concept of judicial review is seen as a key element of the rule of law. According to Paul Scott, 'One of the principles most dear to the UK's constitution is the rule of law, at the core of which stands the requirement that the State abide by law and – a necessary corollary of that – the right of individuals to challenge the lawfulness of the acts of public-decision makers by invoking the supervisory jurisdiction'.[161] However, the

[159] IPT n(114) para 2.8.
[160] *R (Privacy International) v Investigatory Powers Tribunal* [2017] EWHC 114 para 2.
[161] Paul Scott, 'Ouster clauses and national security: judicial review of the Investigatory Powers Tribunal' (2017) P L 355.

IPT is subject to an ouster clause which excludes the exercise of this supervisory jurisdiction. Specifically, section 67(8) RIPA provided that: 'Except to such extent as the Secretary of State may by order otherwise provide, determinations, awards, orders, and other decisions of the Tribunal (including decisions as to whether they have jurisdiction) shall not be subject to appeal or be liable to be questioned in any court'.[162]

Such ouster clauses are generally subject to criticism as they enable decisions of public authorities to escape effective scrutiny. Precluding further review of the procedures of a court or tribunal similarly appears to insulate the procedures of these judicial bodies and is seen as repugnant to constitutional principles.[163] The Courts are generally hesitant to permit such limitations on their jurisdiction.[164] However, the IPT has been held to benefit from such a limitation, thereby insulating their decisions from judicial review. This determination was made in the case of *R (Privacy International) v Investigatory Powers Tribunal* which sought to challenge the 'ouster clause' for decisions of the Tribunal. In holding that the procedures of the IPT were immune from review, Sales LJ placed particular emphasis on the circumstances in which the Tribunal operates.

> Parliament's intention in establishing the [IPT] and in laying down a framework for the special procedural rules which it should follow...was to set up a tribunal capable of considering claims and complaints...under closed conditions which provide complete assurance that there would not be disclosure of sensitive confidential information about their activities.[165]

[162] This clause was described as an 'unambiguous ouster' in *A v Director of the Security Service* [2010] 2 AC 1.
[163] See Laws LJ in the case *of R(A) v Director of Establishments of the Security Service* [2009] EWHC Civ 24 para 22.
[164] *Anisminic v Foreign Compensation Commission* [1969] 1 All ER 208
[165] *Privacy International v Investigatory Powers Tribunal* [2017] EWCA Civ 1868 para 42.

Key to this decision was the specialist subject matter and procedure of the IPT which requires secrecy to ensure that the proceedings before the IPT do not frustrate the aims of the protection of national security or the prevention and detection of crime. Enabling judicial review of the proceedings of the IPT would, according to Sales LJ, subvert that purpose.[166] This must be criticised as it suggests that accepting subversion of the law is preferable and strongly prefers the aims of the State over that of the individual, in direct contrast with core liberal democratic ideals.

The limitation on judicial review, such as that enabled in the decision of *Privacy International*, was argued not to run counter to constitutional principles and the rule of law due to the nature of the IPT and its statutory remit. As Mark Elliot notes, 'the *Privacy International* case did turn out to be an instance of Parliament using language so clear as to displace judicial review: but critically, the conclusion that it had deployed such language was reached only against the background of the judicial view which prevailed in the case to the effect that the ouster was not constitutionally egregious'.[167] Further, the qualifications of those sitting on the Tribunal, namely that they were judges of at least High Court standing, furthered the argument that the IPT was itself exercising standards of review at least comparable to the High Court.[168] However, even in his ruling, Sales LJ was cognisant of the fact that the prevention of judicial review of decisions raised serious concerns. He acknowledged that 'a provision which isolates a tribunal from any prospect of appeal through to this court and the Supreme Court on points of law which may be controversial and important ... involves a substantial inroad

[166] *Ibid* para 43.
[167] Mark Elliot, 'Through the Looking Glass? Ouster Clauses, Statutory Interpretation, and the British Constitution' (2018) University of Cambridge Legal Studies Research Paper 4/2018, 13.
[168] *Privacy International* n(165) paras 41-42.

upon usual rule of law standards'.[169] As such, the inability to demand judicial review of the IPT does not in itself result in a determination that the IPT is an ineffective mechanism for oversight. However, when coupled with the other provisions concerning disclosure and closed procedures it does further demonstrate the lack of transparency of this mechanism. Furthermore, it poses a threat to the basic values enshrined by the rule of law. Immunising the decisions of the IPT from judicial review creates a situation where the IPT can fail to comply with a statutory procedural requirement in reaching a decision that impacts on the rights of a complainant but cannot be corrected by a court. Further, it is another area that makes it more difficult for individuals to seek effective remedies for violations of their fundamental rights which occur through actions undertaken by public authorities.

However, whilst the decisions of the IPT remain impervious to judicial review, the IPA has, for the first time, included a provision that allows individuals to appeal the finding of the IPT to a domestic court. Prior to the 2016 Act, individuals had no further rights barring ultimate appeal to the European Courts. Such a policy ran counter to the ideals of transparency. 'Where there is no possibility of challenging the alleged application of secret surveillance,..., widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified'.[170] The lack of a right of appeal was highly criticised during the various reviews of the investigatory powers instruments. David Anderson, in calling for the institution of a right to appeal, noted that, 'the IPT is unusual in being subject to no process of appeal, an incongruous state of affairs given that it is the only appropriate tribunal for certain categories of human rights appeals and that it can decide issues of great general importance involving

[169] *Ibid*
[170] *Kennedy* n(13) para 124 and *Szabo* n(9) para 36.

vital issues of principle'.[171] As a result of these criticisms, a domestic right of appeal on decisions and determinations by the IPT was introduced under the IPA.[172]

This provision permits appeals to the Court of Appeal 'in circumstances where there is a point of law that raises an important principle or practice, or where there is some other compelling reason for allowing an appeal'.[173] It remains to be seen how this will be interpreted in practice as the wording does not confer a clear right of appeal to ensure the IPT acts in accordance with the law. In order to obtain leave for appeal, an applicant must apply to the Tribunal, no later than 21 days following the provision of the determination or decision of the Tribunal to the applicant.[174] Upon receiving that application, the Tribunal will decide whether or not to grant leave to appeal. Such a decision will be made utilising a procedure similar to that of the second-tier appeals test as set out in s 13(6) of the Tribunals, Courts, and Enforcement Act 2007 which examines first, whether the appeal would raise some important point or principle, or, second, if there is some other compelling reason to hear the appeal. In addition to these criteria, there must also be a determination that the appeal will raise a point of law. If the Tribunal refuses to give leave for appeal, it must provide the parties with a statement of its reasons for refusal and notification of the right to make an application to the relevant appellant court for leave to appeal.[175] In the Impact Assessment for the IPT which considered this domestic right to appeal, the Government noted that the requirements necessary to grant a right of appeal will mean that the power will be exercised sparingly,

[171] Anderson n(45) 14.105.
[172] IPA s 242.
[173] Home Office, *Investigatory Powers Tribunal Consultation: Updated Rules* (September 2017).
[174] IPT Rules n(113) s 16(1).
[175] IPT Rules n(113) s 17(3).

with fewer than ten annually based on the current rulings which gave rise to matters which warranted appeal.[176]

The right of appeal is a necessary check on the decisions of the IPT and one that can increase public confidence in its role as an oversight mechanism. Without a check on the decisions of the IPT, its effectiveness in ensuring individual rights can be called into question; a question that is not helped by the low success rate of applicants. The right of appeal can help to mitigate these concerns. Whilst the right of appeal represents an improvement for individuals in seeking remedies for human rights breaches under the IPA, the closed procedures remain an impediment to the appeal process. To mitigate this concern there should be a presumption in favour of open disclosure which may be rebutted by the public authority if they can provide that there is a greater public interest in preventing disclosure. This would also prevent the blanket application of policies of secrecy that frustrate open justice and would thereby promote increased transparency. The State cannot benefit from the protections of the Tribunal at the expense of the individual. Such an imbalance in power undermines respect for and confidence in the rule of law. Furthermore, enabling judicial review of the decisions taken by the IPT as well as ensuring that the right to appeal is able to be effectively exercised by complainants would strengthen the protections offered by this mechanism. Absent further reforms to the area, the IPT is ineffective to satisfy the requirements that the privacy violations experienced by individuals in the collection and processing of data under the investigatory powers instruments are adequately balanced against the State interests.

[176] Home Office, 'Impact Assessment: Domestic Right of Appeal for the IPT' (7 July 2016) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/538312/domestic-right-of-appeal-from-the-Investigatory-Powers-Tribunal.pdf>.

VII. Applying Contextual Integrity to the oversight mechanisms

As demonstrated in the preceding analysis, the oversight mechanisms which exist under the investigatory powers instruments cannot satisfy the requirement that the use of such powers are in accordance with law, necessary, and proportionate. The current regime cannot counter the impact of the violations of privacy resulting from the retention, access, and analysis of communications data. The context relative informational norms associated with these areas have raised concerns over the nature of the information, the attributes it can reveal, who it is communicated to and why, and who is in charge of the retention, access, and processing of it. Effective oversight needs to address these concerns to ensure that it can provide the needed protections to guarantee privacy in this area. However, the current regime fails to do this. The following looks at the elements of the informational norms which need to be addressed in order to provide an effective oversight regime for privacy. These elements will be incorporated into the prescriptive recommendations for future changes to legislation to be undertaken in the next chapter to guarantee privacy in the collection and processing of communications data in the ICT system.

The elements which fundamentally underpin informational norms are those which are altered in violation of contextual integrity, namely: information types, transmission principles, and actors. With regard to oversight the important attribute of the information is its ability to violate privacy by revealing highly personal information. This is a characteristic satisfied by communications data as has been established in the preceding chapters. Current analysis of interferences with data and the oversight protections ascribed to it largely focus on interception of communications rather than the relevant communications data. The latter must be distinguished from the former.

Communications data has a number of unique features. Principally, the data is expansive and relates to a large proportion of the population, not just those who are relevant to an investigation. As an information type, communications data is seen as less intrusive and therefore it is not required to be subject to the same level of oversight. This is despite the fact that the provisions concerning this type of data cover, in a generalised manner, all means of communications types without differentiation, limitation, or exception. The Courts have accepted that in determining the interference which results from the collection and processing of communications data, consideration must be given to the legislation and the persons who can be affected by it, particularly when the legislation directly affects all users of communications services by applying a blanket policy of interception.[177] Blanket and indiscriminate policies are much more likely to give rise to rights violations. Indeed, the general collection of this information lends itself to the argument that the precedent concerning oversight of targeted interceptions is inadequate to be applied in this context. As was held in the case of *Szabo & Vissy v Hungary:* 'The Court recalls that in *Kennedy*, the impugned legislation did not allow for "indiscriminate capturing of vast amounts of communications" which was one of the elements enabling it not to find a violation of Article 8'.[178] Such an acknowledgement is important and must be taken into account when assessing the oversight mechanisms.

Further, as the powers given to law enforcement regarding this data have increased, so too has the use and flow of this information, thereby altering the transmission principles which dictate how the information is spread between parties. The desire to collect this type of information with ubiquity is a direct corollary to contemporary forms of crime and threats to national security. It is seen as necessary due to improvements in

[177] *Roman Zakharov* n(104).
[178] *Szabo* n(9) para 69.

technology which make it easier for individuals to subvert detection and frustrate investigations. However, this cannot preclude oversight. 'In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens'.[179] Yet oversight in this area remains *ex post* rather than *ex ante*. Oversight only occurring after, and not prior to or during the interferences renders those measures less effective for guaranteeing privacy. It is only with the recent cases of *Digital Rights Ireland* and *Tele2* that the need to have stringent oversight of communications data has been acknowledged. The oversight regime must be modified to explicitly account for these information types and the specific issues they raise. Applying the considerations for oversight which are derived from interception fails to account for the unique nature of this information, ubiquitous and all encompassing, and covering vast swathes of the population. A specific communications data oversight regime is therefore necessary to ensure that the fundamental privacy interests are not violated by these powers.

In addition to shifts in information types and flows, there has been a shift in the powers and functions of relevant actors under the oversight regime. This shift has altered the traditional norms applied to these actors and represents a *prima facie* breach of contextual integrity. Notably, the predominant actors under the surveillance infrastructure have shifted from public to private entities as evidenced in the analysis in Chapters 3 to 5. The communications data provisions are undertaken and facilitated by these private actors who are not subject to traditional accountability measures. The utilisation of private actors to perform the functions regarding communications data

[179] *Szabo* n(9) para 68.

represents an interference with privacy. The European Courts have accepted this position, calling particular attention to the communication of the information obtained by the private actors to public authorities. 'Communication of personal data to a third party, such as a public authority, constitutes an interference with the right to respect for private life, regardless of the subsequent use of the information communicated'.[180] The relationship between public and private actors in this regime creates accountability gaps and privatises sensitive responsibilities.

In order to mitigate the impact of the shift in actors under the communications data regime, oversight must account for the change from public to private, particularly in the collection and retention of data. However, the current oversight regime fails to do so. Significantly, the IPT, which serves as the primary mechanism of relief for individuals, has no investigatory powers where complaints are made about private individuals or companies who are performing functions delegated to them by the investigatory powers instruments. This creates a considerable accountability gap, as even those CSPs who are required, under notice, to collect and process data for law enforcement purposes, cannot be held to account for the human rights violations which occur as a result of these actions. As such, the current oversight regime lacks the capability to provide a check on the powers of one of the dominant actors in the surveillance of communications data. Such a gap is a violation of the traditional norms associated with oversight.

VIII. Conclusion

The preceding analysis has established that the oversight mechanisms provided for in the investigatory powers instruments fail to preserve the context-relative informational

[180] European Agency for Fundamental Rights n(23).

norms associated with communications data. The failings of the existing mechanisms mean that the rule of law is threatened in the use of these powers. There are insufficient checks on the powers of the State to collect and process data that is highly revealing and all-encompassing. Where the balance of interest is weighed, it falls too often in favour of the State at the expense of individual rights. As such, overhaul of the oversight mechanisms is necessary to ensure that privacy is protected from unjust interferences occasioned by the powers of communications data retention, access, and analysis. The following chapter will now set forth prescriptive proposals to ensure that the informational norms associated with the ICT system are protected and that adequate oversight mechanisms are in place to guarantee privacy.

CONCLUSIONS AND PROPOSALS FOR REFORM

I. Introduction

This thesis set out to determine the extent to which the existing legal and policy frameworks surrounding the collection and use of communications data by law enforcement represented a violation of privacy. The preceding chapters have examined the processes by which communications data is retained, accessed, and analysed, and the oversight mechanisms which seek to notionally satisfy the requirements of privacy and the rule of law in these processes. In each instance, developments in the ICT system, associated with their legislative, organisational, and technical components, have enabled the processes to alter context relative informational norms. The development and use of ICT systems for the investigation and detection of crime has been accompanied by changes in the scale and scope of data, classical spatial distinctions, changes in the traditional temporal limits of information, and conceptions of presence in technologically dominated worlds. These changes are not represented in the concept of privacy as it is currently applied to this system. Significant changes in actors and their roles, in information types, and transmission principles, demonstrate that the practices permitted under the investigatory powers mechanisms must be re-evaluated. The current safeguards and oversight mechanisms are insufficient to guarantee privacy and require change. This is necessary in order to prescribe effective reforms to the investigatory powers structure which is the ultimate aim of this thesis. Such prescriptive measures must look at the practices utilised and their resultant impact to determine the best targets for reform.

This chapter will be comprised of three parts. Part I addresses the changes in informational norms which have identified in the previous chapters. This section is

intended to provide an overview of the areas of concern discussed throughout this thesis in order to accurately situate the discussion for future reform. As such, it offers a summary of the findings of how key ICT methods and processes are utilised to pursue criminal justice objectives in a manner contrary to privacy, evidenced throughout the thesis. In presenting these findings, the focus is on the informational norms which exist in the system and values which they reflect. Part II then examines, the overall normative shifts identified within the thesis which have occurred as a result of the use of communications data in the ICT system. This section therefore presents the key findings of the thesis on how the conceptualisation of privacy must be redefined to address these changes and thereby provide for legal instruments which better reflect the technological capabilities and privacy. The normative shifts must be taken into account in order to ensure that the concrete policy changes offered do not suffer from the same failings as their predecessors. In considering the shortcomings of the current system and the normative shifts identified in the two preceding parts, Part III will then offer specific prescriptive recommendations to amend the investigatory powers mechanisms to ensure that privacy will be adequately protected. This section offers an answer to the core question of how to balance privacy rights with the needs of law enforcement in the collection and processing of communications data. Four core recommendations are offered: purpose limitation, data minimisation, increased rights of the individual, and the reclassification of CSPs. Such recommendations are intended to present a better reflection of the informational norms associated with technologies and prescribe a general normative framework of elements that must be considered even in the development of more intrusive technologies.

II. The informational norms and values of the ICT system

The contextual integrity decision heuristic applied to the retention, access, analysis, and oversight mechanisms in Chapters 3 thru 6 indicates that developments in the ICT system have resulted in a breach of contextual integrity. This was evidenced through an analysis of the component elements of the informational norms, namely: information types, transmission principles, and actors/roles. However, the mere indication that informational norms have been altered through the development of the system does not in itself indicate that the new practices are illegitimate. Rather, further analysis is required to determine whether the breach of contextual integrity is justified on the grounds that it better represents social, political, and legal considerations and supports the attainment of the context based values. If the new practices are more effective in supporting or promoting respective values, then the changes in information flows are acceptable.

In order to determine whether this is the case, it is necessary to examine the respective norms and values which exist in the system. These norms are not created through the construction and use of technology nor through legal instruments alone; rather they are derived from interactions between the elements of the system in the legislative, organisational, and technological forms. As Nissenbaum notes, 'to fully appreciate and find norms that are elements of a normative system compelling, one needs to consider them against the backdrop of the system itself. Otherwise, in isolation, they might appear arbitrary or even dubious'.[1] In the context of the system, it is important to note that law and technology are co-constructed. Therefore, any assessment of the normative elements must incorporate the associated dimensions of law, policy, and values which exist within the material and social formations of the technology. These formations play important

[1] Helen Nissenbaum, *Privacy in Context* (Stanford University Press 2010) 140.

roles in the system within which the alleged violations occur.[2] Questions abound as to whether the development of the system supports privacy and its related values such as autonomy, freedom, security, and justice. If so, how are these elements reflected and protected through further developments and uses of the system. As Jasanoff notes, important normative choices are made throughout the life of the system; in 'the phase of emergence; the resolution of conflicts; the classification of scientific and social objects' the standardisation of technological practices; and the uptake of knowledge in different cultural contexts'.[3]

In determining the overall impact on privacy occasioned by changes in informational norms, it is crucial to examine not just how these norms have shifted, but contextualise the use of the ICT system in the different spaces and roles it inhabits, and how that has similarly influenced its development. These contextual factors both mould the production of the technology and enable technological achievements to loop back and shift the organisation of society.[4] To determine how the changes in technology have achieved this in the context of the ICT system, it is necessary to assess the shifts in information flows and the concomitant alteration of informational norms.

These norms are the principles which prescribe acceptable actions in context. In the collection and processing of personal information for law enforcement, these norms have been associated with investigative goals and surveillance. Information about individuals would be collected in the course of investigations; the resultant data could be used to link suspects to crimes or build cases for prosecution. Such information gathering procedures

[2] Barbara Prainsack, 'Unchaining research: processes of dis/empowerment and the social study of criminal law and investigation' in Cloatre and Pickersgill (eds) Knowledge, Technology and Law (Routledge 2014) 76.
[3] Sheila Jasanoff, 'Afterword' in Jasanoff (ed) States of Knowledge: The co-production of science and social order (Routledge 2004) 279;
[4] Jasanoff n(3) 276; Donna Haraway, *Simians, Cyborgs, and Women: The Reinvention of Nature* (Routledge 1991) 183, 201.

were limited, tied to a particular investigation, and typically granted through an independent oversight mechanism. The targeting of surveillance and requirements of additional safeguards provided guaranteed that the measures were legitimate and necessary.[5] However, developments in the ICT system have altered these norms in ways which impact on the overall values of the system and the social goals that they seek to embody.

Within the system, these developments have manifested themselves in changes to the nature of the data, shifts in the nature of borders, and the increasing role played by non-human actors.

a. Changes to the Technical Artefact: Communications Data

In contrast with traditional law enforcement procedures, the developments in law and technology in this system have resulted in the expansion of monitoring of individuals. In part this is a result of individuals being subject to increasing datafication; communications and transactions no longer occur without digital trails. The data in these systems is aggregated and mined for information of value to investigations. As Nissenbaum notes, these processes 'deviate from entrenched practices by enlarging the set of attributes and, possibly, the recipients of aggregated information'.[6] This change in informational norms is apparent in all elements of the ICT system. Data retention and processing has enabled general surveillance and addresses all users of communications services. Such widespread retention, irrespective of suspicion and the seriousness of any alleged crime undermines the legitimacy of the surveillance. The rule of law can be

[5] Jurisprudence in this area further set forth requirements for such surveillance measures to be considered legitimate. See, for example, *Klass & Ors v Germany* App no 5029/71 (ECtHR, 6 Sept 1978); *Kruslin v France* App no 11801/85 (ECtHR, 24 April 1990); *Leander v Sweden* App no 9248/81 (ECtHR, 26 Mar 1987); *Liberty and Others v. the United Kingdom* App no 58234/00 (ECtHR, 1 July 2008).
[6] Nissenbaum n(1) 170.

frustrated by these policies and a disproportionate interference with individuals' fundamental rights can arise.[7]

Historically, this data has been treated as less intrusive than other types of data used in police investigations, such as intercepted communications. This was in part due to the perceived innocuous nature of communications data when these provisions were first being envisaged. Personal ties could be intuited from this information but such relationships could not be conclusively proven without further investigation. However, modern day communications data, due to its expansive nature and ability to permeate all aspects of everyday life, can no longer be readily distinguished from content or treated as less intrusive. Even where retention and processing are considered acceptable, such as when individuals authorise it in order to obtain a particular service, it is purpose limited. The types of information retained are those which people willingly allow to be processed by private companies; they do so in order to be able utilise or customise services. But they do so with the belief that the data that is processed will be used for purposes to which they broadly agree. They do not do so for it to potentially be later used against them in criminal investigations. However, the impact of this is that current policy means that even if behaviour is altered, the data will continue to be retained and processed. 'Increasingly, all that we do in our daily lives involves some form of communications transaction. In so doing, we are subjecting ourselves to surveillance by default, as our activity is retained indiscriminately, preventing us from avoiding such surveillance'.[8] This demonstrates a shift away from the entrenched norms we associate with surveillance and data.

[7] *S and Marper v United Kingdom* App No 30562/04 and 30566/04 (ECtHR, 4 Dec 2008) para 125.
[8] Edgar Whitley Ian Hosein, 'Policy discourse and data retention: The technology politics of surveillance in the United Kingdom' (2005) 29 Telecommunications Policy 857, 869.

The nature of the data and the methods of analysis themselves engage privacy concerns, as processing the data systematically examines personal information in order to determine what is relevant. This sort of systematic processing of information is not traditionally associated with law enforcement; social norms in this area relate to those processes which target individuals under suspicion. Traditionally, certain types of personal information were exempt from these law enforcement procedures, whether due to their sensitive nature or the inability of law enforcement to access them. This is no longer the case. By incorporating CSPs and their data into the analysis processes, information that was previously unavailable can now be used to reverse engineer past, present, and even future breaches through secondary use of the data.[9] The use of this information, from the various data sources, creates categories of individuals that situate populations according to their value, reliability, or risk level.[10]

It is necessary to tightly circumscribe the ends for which this analysis should be permitted. As King and Richards argue, 'We can now do things that were impossible a few years ago, and we've driven off the existing ethical and legal maps. If we fail to preserve the values we care about in our new digital society, then our big data capabilities risk abandoning these values for the sake of expediency'.[11] Ethical and legal guidelines need to take note of the potential intrusiveness of this information in creating an effective framework for governing the use of communications data. In fully assessing the impact of the new methods of collection and analysis facilitated by technology, a balancing exercise must be undertaken. The wider impact of the data and the ability of

[9] Neil Richards and Jonathan King, 'Big Data Ethics' (2014) 49 Wake Forest L R 393.
[10] David Lyon, 'A Sociology of Information' in Calhoun, Rojek, and Turner (eds) *The SAGE Handbook of Sociology* (SAGE 2005) 223.
[11] Jonathan King and Neil Richards, 'What's Up with Big Data Ethics' *Forbes* (28 March 2014) < https://www.forbes.com/sites/oreillymedia/2014/03/28/whats-up-with-big-data-ethics/#e47520435913> accessed 11 Sept 2018.

the analytical tools to intrude farther into the private sphere than previously possible must be taken into consideration. In ascertaining whether these tools meet the necessary requirements of necessity and proportionality, due regard should be had, not only to the individual data itself, but the potential implications which arise through its aggregation and analysis. It is through these tools that the data reveals more about individuals, and therefore, acceptance of their use without an overriding public interest is an interference with privacy.

b. The fluidity of borders within the system

The changes in informational flows resulting from the developments in the ICT system are also reflective of the malleability of traditional boundaries. ICT is not bounded in the manner of other systems. Data flows across jurisdictional spheres. Historically, instruments such as Mutual Legal Assistance Treaties were the mechanisms through which access to data was sought from other jurisdictions. The legislative developments under the investigatory powers instruments now impose direct requirements on CSPs to provide access where the individual or content relates to the jurisdiction, regardless of where it is located. The actors, in the form of CSPs and law enforcement now play different roles in the system, with CSPs performing more investigative functions and law enforcement serving as recipients of data. Legislative developments in this area fail to take this into account, basing their conception of intrusiveness on the social norms which existed prior to these technological developments and failing to consider how social norms have changed because of the technology. When data was limited in the spaces it could be generated and transgress, individual were more likely to be aware of its potential access and use by law enforcement. There were limitations on the extra-territorial effects of the law. Individuals could know the laws of their jurisdiction and be expected to comply; however, with the deconstruction of these traditional jurisdictional

boundaries, this becomes increasingly difficult. Such developments run in contrast to the rule of law and the idea that individuals should be able to know when such legal provisions might be applied to them.

Beyond jurisdictional issues, the ICT system has developed in a way which challenges traditional notions of space. Traditional investigative means are no longer sufficient in light of technology which removes individuals from the traditional spheres wherein they could be physically monitored and investigated. David Lyon argues that the 'integration of different kinds of surveillance is rapidly being enabled by computer networking and the creation of techniques capable of tracing and tracking 'data subjects' behaviour through and between once distinct social realms'.[12] Human surveillance and the use of informers are not effective substitutes for achieving law enforcement aims here. 'As the National Policing Lead emphasised, the alternatives to the use of communications data tend to be more intrusive and to carry both a higher associated cost (in equipment and workforce development) and a higher risk to those deployed'.[13] The legislative elements of the system have developed to facilitate the use of this data to confront this difficulty. Such developments run counter to accepted normative considerations which consider the need for private spheres and spaces free from state intrusion. In removing these boundaries, individuals are subject to increasing encroachment on their autonomy as the spaces wherein the self can be freely expressed and develop become increasingly limited.

[12] David Lyon, 'The new surveillance: Electronic technologies and the maximum security society' (1992) 18 Crime, Law and Social Change 159, 168.
[13] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (Stationary Office 2015) para 9.36.

c. Shifts in the roles of relevant actors

In the development of the system, the roles of human and non-human actors have shifted, with increasing reliance being placed on the non-human elements of the system. Proponents of these developments argue that the increase in automation and removal from the human sphere renders the technology more effective and less prone to the biases which inhibit human action. As Jasanoff notes, 'the hope is that technology, through its mechanical reproducibility, will be impervious to context and will provide unbiased and reliable evidence about the facts of the matter'.[14]

Advocates of removing human actors from the system through technological developments such as Judge Richard Posner hold that these systems confer an impartiality on the processing of personal data and limit the intrusions into personal information and privacy.

> Machine collection and processing of personal data cannot, as such, invade privacy. Because of their volume, data are first sifted by computers which search for names, addresses, phone numbers, etc. that may have intelligence value. This initial shifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read.[15]

Such an interpretation suggests that the fact that the information is processed and analysed automatically by technology implies that it can be removed from undue human influences. Based on this logic, there can be no shift in the entrenched social norms as

[14] Sheila Jasanoff, 'Just Evidence: The Limits of Science in the Legal Process' (2006) 34 J L Med & Ethics 328, 330.
[15]Richard Posner, 'Our Domestic Intelligence Crisis' *The Washington Post* (Opinions 21 Dec 2005) <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html> 17 Jan 2017.

there is no substantive change in who ultimately examines or utilises the data. However, this does not accurately reflect the nature of the information nor the diminish the impact on social norms when this information is retained and processed.

Key to this is the impossibility of the technology ever being fully removed from human influences. This is most readily apparent when algorithms used to perform analysis functions are considered. An algorithm is a mathematical equation which is used to determine a specific result; in this case, the algorithm is used to filter out data which is not relevant to the request (e.g. location data of all cell phones that were not in both specified locations at the specified times). On its face, this would appear to build a neutral element into the filter; however, this interpretation ignores the human role in shaping and developing these algorithms. 'Computer algorithms are written by people, and their output is used by people...Whether or not anyone actually looks at our data, the very fact that (1) they could, and (2) they guide the algorithms that do' has implications for the ability of that processing to constitute an intrusion.[16] Instead of removing the human element, algorithms merely transfer that element into the decision making process itself in a manner that is more opaque.[17]

This lack of transparency is significant as the algorithms and filtering allow for interpretations to be made and meaningful patterns to be found within the data. Indeed, the promise of these technologies is that they can produce predictions of social behaviour, thereby enabling the detection of potential criminals and national security threats. However, the interpretative element calls this into question. Basing these predictions on set categories of data is insufficient to be determinative. This is

[16]Bruce Schneier, *Data and Goliath* (WW Norton & Co 2015) Loc 2007.
[17] Lawrence Busch, 'A Dozen Ways to Get Lost in Translation: Inherent Challenges in Large-Scale Data Sets' (2014) 8 Intl J of Comm 1727 discusses this issue in the context of investment bank traders replaced by an algorithm which did the same work but with relatively less transparency.

exacerbated by the idea that the more any indicator is used, the greater its apparent impact will be, both on users and data subjects, and therefore its importance may become self-reinforcing.[18] As technology is more heavily relied on in investigations, this will become increasingly important. There is a need to ensure that there are no biases in the processes. To fail to do so will potentially cause greater harms to individuals than would occur under traditional investigative means.[19] Further, data analysis can lead to a potential mechanism to squash dissent and target people for other purposes, for example, identifying lead activists or protesters in a movement. 'Suspicious profiles might involve information about people's free speech, free association, or religious activity'.[20] These impact directly on established norms and the interferences, due to their automated nature, are subject to less transparency, less oversight, and offer fewer remedies than their traditional counterparts.

d. The impact on the values of the system

The changes in informational norms indicate that the developments in the ICT system have occurred in a manner which results in an interference with privacy. However, it is necessary to examine whether these changes result in a system which better reflects current social and legal values. 'After all,' as Nissenbaum states, 'in the absence of purpose and drained of teleology, normative practices are little more than empty rituals'.[21] In assessing these values, it is necessary to weigh the benefits for law enforcement in the use of communications data against the interference felt by individuals. It is not enough that there is a legitimate aim in gathering more information;

[18] Campbell's Law as set out in Donald Campbell, 'Assessing the impact of Planned social change' (1979) 2 Eval & Prog Planning 67.
[19] Think for example of the difference between being brought in under suspicion of a crime and later being released when it was discovered that the information leading to your suspicion was incorrect as opposed to the automated process of being put on the 'no fly' list.
[20] Daniel Solove, *Understanding Privacy* (Harvard University Press 2008) 189.
[21] Nissenbaum n(1) 166.

individual rights must be respected as well to ensure that such actions are in accordance with the rule of law and the aims of a democratic society. To balance the aims of the entities involved in the ICT system, it is necessary to examine how the system reflects their values and whether it is weighted disproportionately in favour of one party at the expense of another.

Throughout the thesis the growth and development of the ICT system and concomitant collection and processing powers of communications data has been examined to identify areas where problems arise and how the relevant elements of the system, legislative, organisational, and technical, respond to those problems. The analysis has found that the responses to these problems favour the State, with individuals increasingly being subverted in the process. With regard to the legislative component, the common theme throughout the development of the system has been an increase in the powers of law enforcement to require further retention, easier access, and more revealing analysis. For law enforcement the developments in this area and the statutory provisions which guarantee they can be used enable crime control and the better security of society. By creating surveillance mechanisms which cannot be meaningfully evaded, control can be exercised, ultimately inducing behaviours that are perceived as more socially acceptable.

However, the risks with the legitimisation of these powers are significant. The law is inadequate for the objectives sought to be achieved. As Benjamin Goold summarises:

> Far from being forward looking or progressive, the legislation is instead uniformly backward looking and begrudging. It is hardly surprising that the system of regulation that now operates in the United Kingdom – while detailed and far-

> reaching – is riddled with gaps and lacks any clear set of overarching legal principles or common objectives.[22]

The existence and use of such legislation which allows for blanket surveillance poses a threat to the rule of law. This threat is further exacerbated by the pre-emptive nature of the legislation. The argument is that the data must be retained for its value for future investigations, regardless of whether it relates to an offence that has heretofore been committed. No suspicion is required for the initial retention. This is fundamentally contrary to basic values, including the presumption of innocence. Enabling law enforcement to focus on intelligence gathering and prevention rather than *ex post* investigations shifts their civic function.

The roles of the organisations involved have also shifted dramatically and accountability is made difficult. As Van Brakel argues: 'with the increased use…of surveillance technology it becomes tempting to blame the technology when the risk effectuates itself with the result that no one will be held or feels accountable'.[23] Take for example the developments of new methods for analysis discussed in Chapter 5. If the data allows for new inferences to be made about individuals due to technological developments there is a question of who is responsible for the data as it is then conceived. This is coupled with difficulties which exist in holding CSPs to account discussed in Chapter 6. Individuals cannot challenge these bodies in the same way as traditional public authorities. This is made all the more difficult due to the increased use of these companies to police the online world. The infrastructure of digital society is privately owned, multinational, and

[22]Benjamin Goold, 'Liberty and others v The United Kingdom: a new chance for another missed opportunity' (2009) P L 5, 6.
[23] Rosamunde Van Brakel and Paul De Hert, 'Policing, surveillance and law in a pre-crime society: Understanding the consequence of technology based strategies' (2011) 20 J of Police Studies 163, 178.

segmented. Cooperation from the private sector is fundamental for public authorities to be able to fulfil their duties in this area.

The combination of these factors is apparent in the interaction of the organisations with the legislation which delegates further responsibilities to these organisations. Acting as gatekeepers of the necessary information, the CSPs become agents of surveillance themselves, thereby dispensing with the need for more direct state action.[24] However, the shift in actors cannot be used to usurp the expectations of a traditional democratic society. 'Rule of law obligations, including those flowing from Articles 8 (right to respect for private life) and 10 (freedom of expression) of the ECHR, may not be circumvented through ad hoc arrangements with private actors who control the Internet and the wider digital environment'.[25] Where powers are delegated to private actors to fulfil a state objective, those actors need to be held to account.

> States do not relinquish their international human rights law obligations when they privatise the delivery of services that may impact upon the enjoyment of human rights. Failure by States to ensure that business enterprises performing such services operate in a manner compliant with the State's human rights obligations may entail both reputational and legal consequences for the state itself.[26]

States must require that both their public authorities and the private actors to which they delegate responsibilities are protecting human rights. However, the law must be precise in the way it does this. As recognised by Taddeo and Floridi, 'it is also problematic to ascribe to [CSPs] full responsibility for the fostering and respecting of human rights. For

[24] Uta Kohl, *Jurisdiction and the Internet* (Cambridge University Press 2007) 191.
[25] UNHCHR and CoE, *The rule of law on the Internet and the wider Digital World* (2014) 21.
[26] UNHCHR, *Guiding Principles on Business and Human Rights* (2011 HR/PUB.11.04).

this entails that [CSPs] can arbitrarily and independently decide the circumstances and the modes in which they need to respect such rights'.[27]

The development of the technical elements similarly raises concerns for the system and they themselves become objects for further development or, alternatively, must be constrained to promote normative interests. As Roger Brownsword notes, 'a regulatory environment that is dense with these new technologies is a very different place to an environment that relies on compliance with norms that are either legally or morally expressed or simply implicit in custom and practice'.[28] The impact of the technology is different depending on what technical means are employed. For example, in the context of retention, blanket collection and retention requirements prefer State objectives over that of the individual. These retention policies are embodied through the architecture of the technology. This architecture, comprised of both software which identifies and processes the data for collection, and hardware in the form of servers and infrastructure to store and maintain that data, is dictated by the legislation. Similar technical elements can be identified in the access and analysis areas. Access requests are undertaken utilising workflow software which translates the requests and pulls the necessary information from the relevant servers.[29] Subsequent analysis of the data is done through automated processing techniques utilising both hardware and software components. In this way, the government regulates the conditions under which the targeted activities occur through the infrastructure of the technology.[30] Leenes and Koop, discussing these powers with regards to interception, found that 'governments have passed legislation that

[27] Mariarosario Taddeo and Luciano Floridi, 'The Moral Responsibilities of Online Service Providers' in Taddeo and Floridi (eds) *The Responsibilities of Online Service Providers* (Springer 2017) 26.
[28] Roger Brownsword, 'So What Does the World Need Now? Reflections on Regulating Technologies' in Brownsword and Yeung (eds), *Regulating Technologies* (Hart Publishing 2008) 25.
[29] Interview with Robin Wevell, Head of the IOCCO, Home Office (June 2016).
[30] Lessig refers to this as Regulation through code. Lawrence Lessig, *Code 2.0* (2 edn, Createspace, 2009) Loc 1304.

requires technology providers to build in certain features related to legal norms'.[31] The same is true of the communications data processes.

By embedding the legal requirements within the technical elements, the State is able to further delegate responsibilities to the organisational elements of the system. As Reidenberg summarises, 'infrastructure design offers the state an *ex ante* means to assure that policy decisions are enforced. States can require that rules for the treatment of information be embedded within the technical system architecture. By 'hard-wiring' particular rules within the infrastructure, states preclude violations and automate enforcement of public decisions'.[32] The effectiveness of this as a means for regulating behaviour is enhanced by the inability to evade the technology. As has been discussed throughout this thesis, communications data is generated at a mass scale and with an all-encompassing scope. It is impossible to communicate without generating some form of communications data. Mandating a technological design which provides for the collection and processing of this information in essence requires that individuals interact with the mechanism. Rowland *et al* note that this 'generally leaves users no choice whether to comply with the law or not, because they are physically prevented from non-compliance'.[33]

However, removing the ability of individuals to make decisions to comply with the law raises concerns over moral, social, and political issues. With regard to the former, Brownsword comments that 'a fully techno-regulated community is no longer an operative moral community…[If] techno-regulators know how to stop us from being bad

[31] Bert Jaap Koops and Ronald Leenes, '"Code" and the Slow Erosion of Privacy' (2005) 12(1) Mich Telecom & Tech L R 335.
[32] Joel Reidenberg, 'States and Internet Enforcement' (2003-2004) 1 U Ottawa L & T J 213, 218.
[33] Diane Rowland, Uta Kohl & Andrew Charlesworth, *Information Technology Law* (4th edn) (Routledge 2012) 8.

only by, at the same time, stopping us from being good, then ordinary law for all its imperfections, has something going for it'.[34] Furthermore, utilising architecture and code as a mechanism to ensure compliance and better enforcement of law lacks democratic legitimacy and undervalues the public interest.[35] Any requirements to build technical infrastructure for communications data under the ICT system must incorporate these technical elements but the use of these elements cannot usurp the rule of law or fundamental values of a democratic society. As was recognised by Eggenschwiler, 'the excess and coming together of technical and non-technical issue areas can severely complicate accountability structures'.[36] In order to provide for effective accountability in this area, it is therefore necessary to take both the technical and non-technical into account and determine how they directly impact on norms and values. This requires prescriptive measures which are better adapted to the particularities of the issues that arise from the development of the system.

III. Addressing the changes in informational norms in the ICT system to better reflect privacy

Melvin Kranzberg's first law of technology is that it is neither good nor bad; nor is it neutral.[37] Technologies will amplify the ideology and reinforce the norms of those who develop it and direct its growth. Outside elements, when they possess significant will and influence, can impose their own objectives on the technology and intensify its effects. This has occurred with the ICT system. In order to understand the significance of the technology for privacy, it was necessary to reconceptualise privacy in a context

[34] Roger Brownsword, 'Code, Control, and choice: Why east is east and west is west' (2005) 25 Legal Studies 1.
[35] Chris Marsden & Ian Brown, *Regulating Code* (MIT Press 2013) 170.
[36] Jacqueline Eggenschwiler, 'Accountability challenges confronting cyberspace governance' (2017) 6 Internet Policy Review 3, 5.
[37] Melvin Kranzberg, 'Technology and History: "Kranzberg's Laws"' (1986) 27(3) Technology and Culture 544, 546.

relative manner. This required an examination of the impact of changes in context relative informational norms, precipitated by changes in information types, transmission principles, and actors, in the context of the ICT system which has been at issue in this thesis. In finding that the ICT system is reflective of a co-constructed relationship between law and technology and that relationship is currently inadequate in guaranteeing privacy rights, the question became how to best guarantee social norms in the system. The system itself embeds its own ethical values and norms in a wide variety of areas, including accountability, social connectivity, security, and privacy, among others. These norms, embedded in the system, tend to reflect historic practice, rather than account for the impact of the changes which have been wrought by the development of the system; in the context of ICT, this means that the system embodies entrenched norms rather than those which are context relative. This creates concerns as these entrenched norms are then hard to change.

As the thesis has established, applying entrenched norms in the wake of technological developments is insufficient to guarantee privacy. New norms which better reflect the nature of the technology must direct the development of future legislation in this area; this thesis has identified key areas wherein these normative shifts are evident in the context of communications data. Notably, it is through acknowledging the significance of these normative changes that privacy can be best incorporated and protected within the system. It is necessary to utilise privacy in a manner which is cognisant of the impact of these developments and the context in which it is used. As demonstrated in the preceding chapters, the shifts in information types, transmission principles, and actors alter context relative informational norms and thereby violate contextual integrity. The violations of these norms fall into several categories which must be addressed in the substantive prescriptive measures imposed: scale/scope, spatial, temporal, and visibility.

Any policy recommendations must consider the significance of the changes in these areas in order to protect privacy.

A. Scale/Scope

The amount of communications data generated and the breadth of the areas which it covers has fundamentally altered how we think of that information and the typical norms we assign to it. The most common technologies used by individuals, i.e. mobile phones, laptops, tablets, etc. produce a steady stream of this information, to be potentially collected and processed. Indeed, the technical capabilities of these devices place vast quantities of potentially very revealing personal information directly in to the hands of individuals. The records kept on smartphones of persons contacted, locations visited, and websites searched, provide a thorough record of the most intimate aspects of an individual in small, portable devices. As recognised by Justice Sotomayor of the United States Supreme Court, this data is capable of producing 'a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations'.[38] Prior to this technological development, amassing this level of information would have required multiple persons monitoring the actions of the individual constantly. The comprehensive amount of information which is generated is done so on a scale and with a speed not previously possible.

As demonstrated in Chapter 3, CSPs in the United Kingdom are under obligations to retain this information. However, such notices to retain are placed under a duty of confidentiality which requires that they do not disclose to their users that the information they are generating will be retained per this legislation. Even if individuals were able to

[38] *Riley v California* 134 SC 2473 (2014) para 9.

exercise their own discretion in selecting a provider that they believed would not be beholden to the retention demands, they cannot similarly control whether their correspondents would be equally discerning.[39] As such, the data of the discerning user may still be caught as it would be retained as a record of communication with their colleague. The inescapable nature of the surveillance promoted by the expansive scale and scope of communications data raises fundamental concerns for a democratic society. Furthermore, the permissive access capabilities which apply to this category of information allow it to be used more readily by law enforcement. Analytical techniques are heightened by the mass amounts of data that can now be processed and filtered to derive more meaningful information for investigators. The scope of such information creates the potential for new harms. As Professor Chris Marsden recognised: 'It is extremely difficult to calculate the probability of harm that results from a single disclosure, let alone the cumulative impact, and what data could reveal when combined with a large number of other possible data sources'.[40]

The abundance of information which exists shifts traditional power relationships. Individuals lose access and control over their data and the ability to decide when to engage with various institutions in society. Power rests with those who can access data and possess the abilities to capture, store, and process it at scale.[41] In the ICT system, these actors are the CSPs who collect and control the data, and law enforcement who are entitled to access provided a low threshold is met. These entities strengthen their power by demanding that the pool of information they have access to continues to increase. Further expanding the pool of information enables the creation of pre-emptive

[39] Jon Michaels, 'All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror' (2008) 96 Cal L R 901, 914.
[40] Marsden n(35) 54.
[41] Julie Cohen, 'The Regulatory State in the Information Age' (2016) 17 Theoretical Inq L 369, 384.

surveillance strategies, further removing traditional democratic principles from the process. As Van Brakel argues, '[if] you see that information is what you need to solve a problem but you do not quite know what the problem is and you do not know what future events you are going to be responding to, the temptation is to collect all information about all people'.[42] Yet despite the desire to exploit the volume of communications data generated by the ICT system, law enforcement must be cognisant of the risk that arises with mass data. Law enforcement may suffer from infoglut, demanding new technologies be developed to analyse the data. Similarly, the volume of the data creates security risks and data breaches which can damage the credibility of the system. Furthermore, the monitoring of individuals via this data fundamentally diminishes trust between law enforcement and individuals. This has direct implications for the relationship between the police and the people they are meant to protect and undermines their effectiveness.

b. Spatial

System developments must further account for considerations of spatial elements which have been fundamentally altered by technology. In the context of communications data, the spatial is triggered in various ways. In generating the data by connecting communicating parties, information is frequently routed across servers which may or may not be confined to the traditional jurisdiction of the state. Even communications between two people residing mere miles apart may transgress borders. As Jennifer Daskal summarises, 'the ease, speed, and unpredictability with which data flows across borders makes its location an unstable and often arbitrary determinant of the rules that apply'.[43] . Furthermore, there is no direct link between individuals and their data; it is

[42] Van Brakel n(23) 179.
[43] Jennifer Daskal, 'The Un-Territoriality of Data' (2015-2016) 125 Yale L J 326, 329.

not physical records in their possession but packets of information in virtual space. This physical disconnect between the user and the location of the data impacts on the normative significance assigned to the data.[44]

In an effort to apply traditional normative restrictions regarding space to data which has become untethered from spatial limitations, the investigatory powers instruments seek to apply restrictions on where the data can be kept. These legislative powers further seek to extend the jurisdiction of the State beyond its borders by enabling it to place obligations on providers whose services transgress the state in some form.[45] This comports with the precedent that if control can be exercised either over an individual or their assets, including, in this case, a CSP, then a court may exercise jurisdiction regardless of where the data is actually located or where the CSP is domiciled.[46] However, this ignores the nature of the technology. Networks do not have fixed boundaries and their expansion or contraction correlates with the interests and values they promote.[47] Companies forced to comply with stricter obligations within the UK in order to facilitate law enforcement under the investigatory powers instruments may chose instead to relocate or alter their networks to frustrate these obligations. This will be particularly true with large multinational corporations who have the infrastructure and capacity to relocate to jurisdictions that better align with their business needs.[48]

Applying regimes which seek to enshrine norms associated with traditional spatial bounds will therefore not work in this context. Rather, spatial constraints need to be reconsidered. Manuel Castells argues that 'rather than looking for territorial boundaries,

[44] *Ibid.*
[45] The proposition in the IPA for this is either/or. Jurisdiction can be applied where the individual of interest is in the State, where the data of interest is in the State, or where the CSP is located in the State.
[46] Andrew Woods, 'Against Data Exceptionalism' (2016) 68 Stan L R 729, 736.
[47] Manuel Castells, *Communication Power* (Oxford University Press 2013) 19.
[48] Michael Kirby, 'New Frontier: Regulating Technology by Law and 'Code'' in Brownsword and Yeung (eds), *Regulating Technologies* (Hart Publishing 2008) 382.

we need to identify the socio-spatial networks of power that, in their intersection, configure societies'.[49] This requires an understanding of the networks, how they are built, function, and connect with one another as assemblages. According to Saskia Sassen these assemblages are neither global nor local but both simultaneously.[50] Castells defines this as the space of flows which allows for social continuity without territorial congruity.[51] This allows for a consideration of the social beyond the traditional confines of the state. To fully understand the impact of the collection and processing of communications data the impacts need to be understood beyond the territorial bounds within which they occur.

c. Temporal

The entrenched norms associated with the use of data by law enforcement have also been fundamentally altered by temporal changes. This has been evidenced throughout the thesis by reference to the powers which enable not only retrospective, but also pre-emptive policing techniques. The wider significance of this and the development of the capabilities of the ICT system more generally is a fundamental shift occasioned by the development of the technology to the nature of time. With technology, time can become compressed. Communications and interactions can occur instantaneously. When an email is sent, it can be received and read by the end user within seconds. The same can be said of a text message.

The communications data associated with these transactions is a representation of the compression of time through technologies. For Castells these communication

[49] Castells n(47) 18.
[50] *Ibid.*
[51] Manuel Castells, 'An Introduction to the Information Age' in Webster (ed) *The Information Society Reader* (Routledge 2004) 138.

technologies allow for the annihilation of time and the elimination of the known sequences of past, present, and future.[52] Relatedly, the capabilities to retain and store information removes ephemerality from society. As Leenes and Koop note, 'the continuous localisation offered by current and future technologies thus significantly contributes to the 'disappearance of disappearance' that is a defining characteristic of the information age'.[53] The change in the temporal resulting from the development of the ICT system is not adequately reflected in the legislation. The permanence of data and the immediacy with which it can be accessed alter law enforcement processes. In particular, the ability of the individuals to challenge access requests are defeated by the speed with which information is conveyed to law enforcement. The investigatory powers instruments do not take this into account in dictating the limits and constraints of the provisions concerning access. Nor are they addressed in any oversight mechanism. Such a shortcoming must be provided for in subsequent legislation.

d. Visibility/Presence

Closely aligned with the preceding categories of norms which have been fundamentally altered as result of the development of the ICT system are the interrelated concepts of visibility and presence. These concepts relate to the ability of the individual to be 'known' based on the communications data generated. As Gillespie explains, 'the most knowable information (geolocation, computing platform, profile information, friends, status updates, links followed on the site, time on the site) is a rendering of that user, a "digital dossier" or "algorithmic identity" that is imperfect but sufficient'.[54] The nature of communications data is comprehensive. It produces digital selves of individuals that

[52] Castells n(51) 145.
[53] Koops n(31) 341.
[54] Tarleton Gillespie, 'The Relevance of Algorithms' in Gillespie Boczkowski and Foot (eds) *Media Technologies: Essays on Communication, Materiality, and Society* (MIT Press 2014) 167, 173.

are representative of information that is deemed relevant to law enforcement. Yet there is a disconnect between this information and the 'self'. As the information collected is only that which is deemed relevant to the law enforcement aims, it does not create a single identity. Rather there is a multiplication of identities which become disconnected from the self, yet, reconnectable when deemed necessary.[55]

Such a separation of the information from the individual means that law enforcement does not ascribe the same protections to that information as they would to a known individual. Yet it is not sufficient to claim that the data means the individual should be removed. Individuals and their discrete data cannot be so easily divorced and any prescriptive changes to the law needs to take this into account. To fail to link the data and the 'self' results in privacy being easily sacrificed for the needs of law enforcement. After all, if it is seen as a mere factum or piece of information rather than a potentially revealing aspect of the 'self', then the individual interest in privacy can easily be subverted to the aims of law enforcement. As Vincent Miller remarks, 'if we are to retain any sense of privacy…we also need to recognise the nature of contemporary selves and their non-material assemblages, and thus consider expanding the notion of 'self' legally and in ethical practice, to include the presences we achieve through technology'.[56] The acceptance that discrete units of communications data can still trigger privacy concerns as they can be tied to the embodied lives of persons must be acknowledged if future legal instruments are to comport to the necessary informational norms.

The technological developments which alter entrenched norms concerning data's scope and scale, spatial confines, temporal limits, and the notion of the self must be reflected in the prescriptive recommendations to amend the investigatory powers instruments.

[55] Lyon (ed) *Theorizing Surveillance: The Panopticon and Beyond* (Willan Publishing 2006) 335.
[56] Vincent Miller, *The Crisis of Presence in Contemporary Culture* (Sage 2016) Loc 2354.

Failing to account for the changes in these norms means that the legislation will continue to violate contextual integrity in a manner that represents a distinct privacy intrusion. Practical recommendations for amendments to the legislation which can better ensure that these normative ideals are considered will now be discussed.

IV. Recommendations for future developments to address the issue of privacy in the collection and processing of communications data

The question becomes what practical policy recommendations can be implemented to account for the shortcomings identified throughout the thesis regarding the collection and processing of communications data. The following prescribes substantive measures which take into consideration the changes in context relative informational norms and can better protect privacy in the context of the ICT system and this data. Such recommendations address a key contribution of this thesis, namely prescribing an alternative legal regime for communications data which protects privacy.

a. Purpose Limitation

The most fundamental change to the investigatory powers instruments which must be undertaken is to limit the purpose for which the data may be retained and accessed. Specifically, communications data should be retained, analysed, and accessed solely for the purpose of preventing, investigating, or detecting 'serious crime'. 'Serious crime' is a subjective term and therefore requires defining. Across the EU there is no single definition of 'serious crime'. Some Member States define it with regard to a minimum prison sentence; to the possibility of a custodial sentence being imposed; or with regard to a list of specific criminal offences.[57] Still other Member States refer to 'serious crime'

[57]European Commission, *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)* (18.4.2011, COM (2011) 225 final, 2011) 6. Ten Member States define 'serious crime' in this manner:

without defining it.[58] Several domestic statutes in the UK make reference to 'serious crime' and can offer further guidance as to the elements which define the term. Under the Police Act 1997, 'serious crime' is defined as that which involves the use of violence, results in substantial financial gain, or is conducted by a large number of persons in pursuit of a common purpose.[59] With regard to the investigatory powers instruments, 'serious crime' was originally defined in the Interception of Communications Act 1985 section 10(3). Therein it was held that conduct would only meet this threshold if '(a) it involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose; or (b) if the offence or one of the offences is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more'. This definition was retained under section 81(3) RIPA and subsequently under s 263 IPA.

Whilst 'serious crime' is defined in the IPA, it does not currently apply to the provisions regarding communications data; rather its restrictions pertain to those powers under the Act for which a warrant is required: namely, interception of content, equipment interference, bulk interception warrants, and bulk personal dataset warrants. This is in direct contradiction to the CJEU ruling in *Tele2 and Watson* wherein it was held that 'Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting 'serious crime' is

Bulgaria, Estonia, Ireland, Greece, Spain, Lithuania, Luxembourg, Hungary, the Netherlands, and Finland. For example, in Ireland, 'serious crime' is defined in relation to offences punishable by imprisonment for a term of 5 years or more. [Communications (Retention of Data Act) 2011 Article 6.]

[58] This is the case for Malta, Portugal, and the United Kingdom which merely state: for the investigation, detection, and prosecution of 'serious crime'. European Commission n(57).

[59] Police Act 1997 s 93(2)

capable of justifying such a measure'.[60] The Court went on to say that the *targeted* retention of data for this purpose could be met provided that the retention was limited to what was strictly necessary.[61] The use of the term targeted retention here is telling. In the judgment, the Courts frequently referred to the powers at issue as blanket data retention. The specific allusion to targeted retention as the type of retention which could be justified indicates that the Court believed there should be specific limits. Indeed, in *Tele2* the CJEU provided an example of what those limits might be, for example, 'using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences'.[62] The ruling in *Tele2* made clear that the requirement of 'serious crime' should be applied to retention policies. The case of *Tele2 and Watson* further went on to establish that access to the retained data should also occur only if the 'serious crime' threshold was met.[63] However, in implementing the ruling of *Tele2 and Watson* the Court of Appeal held that the regime at issue was in violation in that it did not constrain access to cases which involved 'serious crime'.[64]

It is notable that the ruling in the domestic courts did not interpret the retention provisions in the same manner as the CJEU. By constraining the limitation to 'serious crime' to access, the ruling permits the retention policies to continue and potentially expand. This certainly comports with the police aims in this area as any limitation on their power to retain and access communications data frustrates their aims. Even limiting access to this data in line with the requirement that it meet the 'serious crime' threshold

[60] See also Joined Cases C-293/12 and C-549/12*Digital Rights Ireland v Minister for Communications & Ors and Michael Seitlinger & Ors* [2014] 2 All ER; *Joined Cases C-203/15 Tele2 v Post-och telestyrelsen & C-698/15 Watson & Ors v Secretary of State for the Home Department* (2016) ECLI 970 para 102.
[61] *Tele2* n(60) para 108.
[62] *Tele 2* n(60) para 111.
[63] *Tele* 2 n(60) para 125.
[64] *Watson v SSHD* [2018] EWCA Civ 70 para 27.

is seen as an action which diminishes police powers. The Chief Constable of Gloucestershire Richard Berry described the law enforcement view on this, 'Crimes may not meet the threshold for "serious crime" but they matter to the people and communities who fall victim to them; solving and preventing these crimes is at the very heart of what [the police] do'.[65] The hesitancy of law enforcement to apply a 'serious crime' threshold was apparent in the evidence offered during the Bill stages of the IPA. Therein a survey was undertaken to establish the common perception of what defined 'serious crime' amongst law enforcement. It was found that 'law enforcement is not able to define 'serious crime'. Most definitions that are used are very subjective and what may be classed as serious to one victim may not be serious to another'.[66]

Despite the opposition of law enforcement to constrain their powers to instances of 'serious crime', current proposals to amend the IPA do seek to implement this distinction as it regards access to communications data.[67] The Government proposals would distinguish between accessing 'entity data' and 'events data'. 'Entity data' is similar to 'subscriber information'. It concerns phone numbers or other identifiers linked to a device, the physical address provided to a CSP, and IP addresses linked to individuals.[68] The Government alleges that this type of communications data is less intrusive and therefore a 'serious crime' provision would not have to be met for law enforcement to access this information; rather, the data could be accessed for the previous purposes of preventing or detecting any crime or preventing disorder.[69] The 'serious crime' provision

[65] Richard Berry, 'Updating our investigatory powers matters for day-to-day crime too' (*The Telegraph* 17 Oct 2016) <http://www.telegraph.co.uk/news/2016/10/17/updating-our-investigatory-powers-matters-for-day-to-day-crime-t/> accessed 4 Feb 2017.
[66] Joint Committee, *Investigatory Powers Bill Witten Evidence,* Law Enforcement Submission Annex E 9; It is interesting here that the focus is on the victim rather than the act. This would seem to indicate that there is a tendency for 'serious crime' to be associated with result crimes rather than conduct crimes.
[67] This is all the more pressing following the ruling of *Liberty v SSHD* [2018] EWHC 976 on April 27 2018 which set a deadline of November 1st 2018 to implement the 'serious crime' limitation into the legislation.
[68] IPA s 261(3).
[69] Home Office, *Government Consultation on the Investigatory Power Act* (November 2017).

would then apply to requests to access 'events data'. This is data that identifies events taking place on a telecommunications network at a specific point in time and space.[70] This would include for example, call records, text message records, data concerning messages sent via non-traditional CSPs (WhatsApp, Facebook, etc.), and location data. The reasoning behind this, argues the Government, is that 'events data' is more revealing than 'entity data' and would therefore be subject to the 'serious crime' limitation. In practice, it is difficult to separate these two categories of data and difficult to see why the blanket retention and access to one should be provided at a lower threshold than the other.

A further concern arises when the proposed definition to be applied to 'serious crime' is considered. As per the Government proposals, 'The new "serious crime" threshold is defined as an offence for which an adult should be capable of being sentenced to six months or more in prison, an offence by a person who is not an individual, or an offence which involves the sending of a communication'.[71] Such a definition considerably lowers the threshold for what makes a crime 'serious'. It cannot be perceived as a meaningful reform of the current framework which has been held to be unlawful. There will be very few criminal offences which do not fall under this definition. Indeed, the Home Office stated that in practice the only offences that would not be included in this definition would be 'summary offences'.[72] While the proposals for reform to the IPA appear to try to meet the letter of the law they do not meet the spirit with which it was intended. Nor do they offer any additional protections which are necessary to protect

[70] IPA s 261(4).
[71] Home Office n(69) 6.
[72] Liberty, *Response to the Government's consultation on the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data* (18 Jan 2018) < https://www.libertyhumanrights.org.uk/sites/default/files/2018.01.18%20liberty%20consultation%20response%20FINAL.pdf> accessed 4 Feb 2018, 6.

against the undue privacy intrusions which result from this data. For true reform to be offered, in line with the principles set forth by the CJEU rulings, further action is required.

Namely, the definition of 'serious crime' must at least meet the threshold of existing definitions of 'serious crime' in the current Acts. There is no reason why the threshold of a minimum three-year sentence in the context of interception cannot be applied to communications data. As discussed throughout this thesis, communications data can be just as, if not more revealing, than that of the content derived from an interception. Furthermore, the distinction between 'entity' and 'events' is impractical. Both categories of data are revealing and their retention triggers privacy intrusions. Distinguishing between the two adds unnecessary complexity to the issue. Access to all categories of communications data should be required to meet the same 'serious crime' threshold.

An interrelated issue in defining 'serious crime' is the blurring of distinctions between activities that would fall under this threshold, and those that fall under the remit of national security. The State is afforded a wide margin of appreciation in cases of national security and the Courts have recognised this. Where national security is at stake, data access provisions may be broadened to people other than the specific targets.[73] However, permitting this additional access must be based on objective evidence that the data will contribute to the fight against a specific national security threat. In countering these national security threats, enhanced cooperation between law enforcement and security and intelligence agencies is required; yet there must be strict organisational separation between law enforcement and intelligence agencies.[74] The interactions

[73] European Union Agency for Fundamental Rights, 'Surveillance by Intelligence services: fundamental rights, safeguards, and remedies' (2017) Vol 2, 22.
[74] This is the case in the UK; other EU Member states fail to provide for strict organizational separation of intelligence and law enforcement, including Austria, Denmark, Finland, and Ireland where the body

between the two become embedded in the processes they undertake. Law enforcement becomes increasingly pro-active and focused on preventative policing and investigating future threats. Intelligence agencies are, for their part, increasingly assigned a role in tackling relevant 'special crimes' beyond those that solely represent a threat to national security, such as online child abuse.[75]

The concern that arises in the blurring of the distinction between national security and 'serious crime' is that the increased powers and wider margin of appreciation afforded to issues of national security may gradually be extended to lesser crimes as well. In the case of data collection and processing as discussed in this thesis, national security is often used to justify more intrusive and enhanced powers.[76] However, this term is loosely defined. It is a 'protean concept designed to encompass the many, varied and (it may be) unpredictable ways in which the security of the nation may best be promoted'.[77] As the definition is vague and capable of being easily extended it poses a threat to fundamental principles of the rule of law. 'Given the increased partnerships between law enforcement and intelligence and security agencies, this negation of the rule of law threatens to spread from the latter to the policeman and prosecutors'.[78] In order to counter the threat to the rule of law which exists from the use of the national security exception for data collection and processing powers, claims that information concerns national security must be subject to rigorous scrutiny.

---

responsible for intelligence activities is officially part of the police and/or law enforcement authorities. [*Ibid* 28].

[75] Douwe Korff et al, 'Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes' (Legal Studies Research Paper Series, University of Cambridge Paper No 16/2017) March 2017, 27.

[76] This takes the form of permitting these agencies to retain bulk data sets and process that data *en masse* to find targets of interest. Profiling and filtering takes place at scale. Furthermore, powers can be granted to interfere with equipment allowing these Agencies to access individuals' devices and the information within. The oversight provisions in this area are even more opaque than those concerning law enforcement access.

[77] *Secretary of State for the Home Department v Rehman* [2003] 1 AC 153

[78] UNHCHR and CoE n(25) 19.

If the powers are to be exercised under the national security exemptions, the State should first prove that the threat cannot be met by processes of ordinary criminal law. This needs to occur through a judicial or at least independent process. As McIntyre notes, the judiciary are best placed to make these assessments and 'consider whether measures which appear desirable in the short term are in accordance with law and – in the last resort – whether they are compatible with the longer term interests of a democratic society'.[79] Cases which blur the distinction between national security and 'serious crime' need to critically assess whether the acts or threats under investigation truly fall under the national security ambit. Furthermore, any claims that the use of the powers are for the purposes of national security must be subject to some threshold of proof. This is particularly relevant for the IPC and IPT to be able to fully fulfil their duties. Any application or notice that is issued under the IPA for the purposes of national security must receive thorough scrutiny and evidence must be offered by the State to prove that the wider powers permitted by this reasoning are thus necessary. As Solove notes, 'national security is a nebulous concept that too often is used to justify decreased regulation, oversight, and accountability'.[80] Subjecting claims of national security to scrutiny would enhance the legitimacy of actions taken on foot of these claims and further ensure the rule of law is upheld. As then Independent Reviewer of Terrorism Max Hill QC stated, 'Suggestions…that human rights prevent the police from fighting terrorism are misguided…Human rights exist to protect us all. Weakening human rights protections will not make us safer'.[81]

[79] TJ McIntyre, 'Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective' in Scheinin Krunke and Askenova (eds) *Judges as Guardians of Constitutionalism and Human Rights* (Edward Elgar 2016) 3.
[80] Daniel Solove, *Nothing to Hide: The False Trade-off Between Privacy and Security* (Yale University Press 2011) 69.
[81] Max Hill, Independent Reviewer of Terrorism Legislation; 'Rights vs Security: the challenge Engaged' (24 Oct 2017) Tom Sargant Memorial Lecture for JUSTICE.

b. Data Minimisation

In addition to limiting the purposes for which data can be retained and used, another method to better protect privacy under the investigatory powers instruments is the minimisation of data collected and accessed. As noted throughout the thesis, communications data is generated through interactions, whether they occur via telephone, online, or even via post. The connectivity of individuals and frequency of communications means that the amount of data which falls under the definition of communications data is increasing exponentially. This information is spread across platforms and networks. Data minimisation emphasises collecting less data *ab initio.* This can be achieved through the infrastructure, in the form of software and hardware which creates and utilises the data, and also by reliance on legal principles.[82] Such data minimisation can promote privacy by preventing personal information from being circulated.

With regard to changes in infrastructure, system design should incorporate data minimisation aims. For example, certain categories of data must be explicitly excluded from the scope of the data retention provisions. These provisions should not mandate the retention of any categories of data which are not generated by the CSP in the ordinary course of their business. This is not currently the case, as categories of data, such as ICRs, are retained under the current legislation. This requires additional infrastructure on the part of the CSP and the processing of more data to meet these aims. These provisions, and any further recommendations to expand the categories of data required

[82]Lilian Edwards, 'Privacy and Data Protection Online: The Laws Don't Work?' in Edwards and Waelde (eds) *Law and the Internet* (Hart 2009) 468.

under the investigatory powers instruments should be subject to increased scrutiny and where possible rolled back. As technologies develop there will be new and increasing amounts of data and ways for law enforcement to potentially use that information. However, this raises the threat to privacy and cannot be done in a blanket manner which promotes the collection and processing of personal data over individual rights. Further, strategies to permit data minimisation should include technical access requirements which require that multiple persons oversee and authorise the disclosure of the relevant information from the CSP. This will ensure that the information provided is limited to what is necessary. Encryption technologies could be applied to categories of data that cannot be retained or accessed via these instruments.[83] In this case, even if the information were accidentally disclosed, no meaning could be garnered from it without further analysis by the law enforcement authority.

In addition to technical changes to ensure data minimisation, further legal requirements must be instituted. A key method for achieving data minimisation is to subject any retention, access, or analysis provisions to judicial scrutiny which assesses whether the measure is strictly necessary to satisfy the objective and whether it is proportionate to the interference which will result. The aim of this scrutiny is to minimise the data, and consequently, individuals, interfered with and constrain the powers governing communications data. Judicial scrutiny requires the CSPs collecting and providing the data, and the bodies requesting access to that information to more concisely define their needs. With regard to retention, Professor Ian Brown recognised the benefit of this approach, explaining that 'A system for judicially authorised preservation and production orders of communications data stored by Internet Service Providers and other

[83] Germany has instituted some of these techniques in their law on data retention, Vorratsdatenspeicherung Article 113.

intermediaries would avoid the blanket intrusion into privacy of population wide data retention laws'.[84]

Access provisions would similarly benefit from further judicial scrutiny. These requests should be specific and only used when strictly necessary. It is unacceptable to ask for a broad range of data in the hopes of identifying a suspect. Rather, these powers should be used as a corroborative mechanism. Communications data access should not be the first step in the investigative process. Once a suspect is identified, the data may be accessed to further build a case or identify associates. However, even then this power should be confined to what is strictly necessary and the data needs to be limited in its scope.

Furthermore, the use of the information accessed must be linked to a specific investigation and excess data provided to law enforcement must be destroyed. This is not currently the case. The existing Code of Practice permits any excess data disclosed on receipt of a communications data access request in the course of an investigation to be used if an addendum is made to the original application for the data.[85] Furthermore, there must be limits on the sharing of communications data by law enforcement once that information is accessed. Neither RIPA nor the Codes of Practice place restrictions on further disclosure between authorities. Rather, the provisions that exist concerning the sharing of communications data are solely concerned with CSPs. The potential spread of communications data to law enforcement authorities beyond the investigating officer greatly increases the risk of collateral intrusions, data misuse, and violations of privacy. The investigators able to view and utilise the data must be confined to mitigate this risk.

[84] Ian Brown, 'Communications Data Retention in an Evolving Internet' (2010) 19(2) International Journal of Law and Information Technology, 101.
[85] Home Office, *Acquisition and Disclosure of Communications Data Code of Practice* (March 2015) para 6.28.

In order to ensure that the access is limited in its scope, access request must be subject to judicial approval rather than the current process wherein approval by a designated person within the public authority is sufficient. This would allow it to comport with the rulings of the CJEU which made clear that requests to access communications data must be approved by a court of independent administrative body.[86] To address this, the Government is establishing an Office for Communications Data Authorisations (OCDA). This will be a non-judicial administrative body to authorise requests to access communications data. Currently the OCDA is set to begin overseeing access requests in April 2019.[87]

Whilst not much is yet known about the specifics of the Office, some of the information provided does raise concerns about the independence of the Office and its ability to fully satisfy the requirement that authorisations be scrutinised by a judicial or independent administrative mechanism. Much like the IPC, the OCDA will ultimately be responsible to the Home Office. As already criticised in the context of the IPC, this essentially requires the OCDA to oversee the work of its employer and raises concerns over its ability to exercise its powers with full independence. Further, the person specification for applicants to the OCDA requests prior experience working with public authorities or law enforcement.[88] Whilst not necessarily prohibitive, this raises concerns of potential bias in favour of the applicants applying to access the data. There is no requirement that the 'authorising officers' have any legal experience or qualifications. Rather, the only essential qualifications for the post are the ability to analyse and evaluate information and communicate their decisions. Furthermore, the description of the OCDA and the roles of

[86] See *DRI* n(60) and *Tele2* n(60).
[87] Office of Communications Data Authorisations, 'Authorising Officer Candidate Information Pack' (18 May 2018) < file:///C:/Users/amh56/Downloads/676313.pdf> accessed 6 June 2018.
[88] *Ibid.*

those involved focus solely on the importance of communications data for investigations and the ways it will assist authorities.[89] The importance of the individual whose data is being accessed and their privacy is not acknowledged in the information.

The current proposals and information provided for the OCDA do not indicate that it would provide for the independent check on the use of communications data required. In order to fix these shortcomings, any body which approves an access request for communications data must be fully independent of the Home Office. Ideally such a body would be a judicial body, bound to the principles of judicial independence and with a thorough understanding of the limits and requirements of necessity and proportionality. This body could fall under the remit of Her Majesty's Courts and Tribunals Service, the unit responsible for the judiciary in the UK. Furthermore, the individuals who approve or deny the access request should have a background that enables them to fully understand the requirements of necessity and proportionality as prescribed in law. In addition, authorising officers should have a thorough understanding of technical systems and the nature of data as these are key elements to understanding the full scope of the powers and risks to individuals that can arise from illegitimate and unnecessary access to the information. To fail to mandate these requirements means that the OCDA merely provides a veneer of oversight; the systemic issues remain.

c. Rights of the Individual at the IPT

Related to the two preceding prescriptions for purpose limitation and data minimisation is the need for the individual to be brought back in to the process. The capabilities of law enforcement that arise through increased communications data retention, access, and analysis increases the power of the State at the expense of the individual. As Leenes and

[89] *Ibid.*

Koop recall: 'the parties capable of monitoring are usually the people in power, governments or large corporations, who have a vested interest in personal information for various reasons. Since they set the rules, one cannot expect monitoring efforts to decrease'.[90] This poses a risk to the nature of the democratic society. Under the investigatory powers instruments, the role of the individual in the process has diminished; individuals are broken down into discrete units of data and control over that data is removed. The individual lacks the power to challenge the retention of their data and is not informed when that data is subsequently accessed and analysed.

The ability of the individual to exercise their rights by recourse to the judicial process is severely constrained. The only judicial mechanism of record for these powers is the IPT who has limited powers; as such the judiciary is largely side-lined in the process. Even where challenges before the IPT are brought, they are made difficult due to a low awareness amongst individuals about the existence or function of the tribunal; the reliance on assumed facts; the minimal reasoning given for the determination by the IPT; the complexity of the matters; and the fact that legal aid is not available for individuals who seek a remedy in this manner. For privacy to be truly protected, the oversight which guarantees the legitimacy of the privacy interferences which result from the powers under the IPA must be subject to an oversight mechanism that better guarantees individual rights.

A critical step to ensure that individuals can exercise their rights with regard to the IPT is to provide for a right to *ex post* notification of surveillance activities that are undertaken on the basis of the provisions of the IPA. This would allow individuals to better craft their complaints before the IPT and ensure that all those whose right to privacy had been

[90] Koops n(31) 335.

interfered with as a result of their data being retained and accessed could benefit from the oversight of the Tribunal. It would remove the reliance on 'assumed facts' which is currently employed by the IPT. A right to *ex post* notification following surveillance measures exists in other jurisdictions.[91] As early as 1987 the Council of Europe issued Recommendation R(87) 15 requiring the notification of individuals who had been subject to surveillance measures. The United Nations has similarly acknowledged the importance of such a right. 'Individuals should have a legal right to be notified that they have been subject to communications surveillance or that their communications data has been accessed by the State'.[92] The CJEU has similarly recognised that individuals must be notified. In *Tele2* the CJEU held: 'the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities'.[93] The ECtHR has similarly recognised the necessity of these measures.[94] Indeed, the Court has held that the omission of this notification can be regarded as a violation of both Article 8 and Article 13.[95] Permitting *ex post* notification of the individual, once that notification will no longer prejudice ongoing investigations, would help to mitigate the informational disparity that currently exists in the IPT.

[91] Both Germany and Sweden stipulate a notification requirement in cases of general surveillance of communications. See Article 101(4) of the German Criminal Code which requires not only the subject of surveillance be informed but also others who might have been concerned by the surveillance measures.
[92] Frank La Rue, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (UN 2013) A/HRD/23/40 82.
[93] *Tele2* n(60) para 121; see also: ; Case C-553/07 *College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer* [2009] ECLI 293 and Case C-362/14 *Max Schrems v Data Protection* Commissioner [2015] ECLI 650.
[94] *Klass & Ors v Germany* App no 5029/71 (ECtHR, 6 Sept 1978); *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 Dec 2015) para 287.
[95] *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* App No 62540/00 (ECtHR, 28 June 2007).

Despite the advantages of *ex post* notification and its acceptance by international bodies and the European Courts, the UK has declined to institute such a protection under the IPA. As per the Home Office consultation of 2017, which was undertaken to implement the ruling of *Watson*, 'the Government's position is that a general requirement to notify an individual that their data has been accessed would unnecessarily inform criminals, suspected criminals, and others of the investigative techniques that public authorities use'.[96] The Home Office went on to note that due to the large number of authorities able to use the communications data powers, it would be impossible to note when all of the relevant bodies were done with their investigations and use of the data.[97]

These arguments represent a weak justification for why notification cannot occur. The fact that the data is spread widely across public authorities should reinforce the ideas of purpose limitation and data minimisation discussed above. The data should not be shared so widely as to make it impossible to determine what authorities are using it for and when it will no longer be relevant to them. Nor can the fact that it would inform criminals of the investigative techniques be used to justify the absence of the requirement. Particularly when the Home Office report subsequently notes that these criminals will be informed if that data is then used against them as evidence during the criminal justice process.[98] Such a provision offers little oversight or guarantee for those individuals whose rights have potentially been violated. As McIntyre notes, the distinction that such evidence will be disclosed in criminal proceedings means that the oversight is '*ad hoc* in that it depends on whether a prosecution is brought in a particular

[96] Home Office n(69) 20.
[97] Home Office n(69) 20.
[98] Home Office n(69) 21. The Criminal Procedure and Investigations Act 1996 provides that the prosecution must disclose that material which assists the case of the defendant or undermines the prosecution's case.

case and does not necessarily provide any insight into wider practices'.[99] Such a refusal to implement notification is contrary to the established international principles and precedent in the area.

It is accepted that notification may not be possible in all cases but it is submitted that this should be the exception rather than the rule. In order to determine whether the prevention of notification was necessary, the IPT could evaluate the particular circumstances against the requirements of necessity and proportionality. In this way, the powers could be limited where disclosure would threaten national security or the investigation of 'serious crime'. Barring the establishment of an overriding reason for not disclosing the surveillance, the surveillance subject should be notified. In this manner notification can act as a safeguard against abuse. Furthermore, it would provide an essential tool for individuals to seek an effective remedy in cases where they were subject to communications data surveillance.

As was discussed at length in the preceding chapter, individuals who make complaints regarding the use of these powers often lack sufficient information to be able to persuasively make their case. As disclosure of relevant information is precluded and the Tribunal operates in secrecy there cannot be said to be open justice in the context of claims arising under IPA. Such informational disparity and opaque proceedings represent a significant impediment for individuals in securing an effective remedy. Notification offers a much needed corrective to the imbalance of power. Indeed, as JUSTICE recognised in their report *Freedom from Suspicion*,

> It is telling, for instance that the IPT's most notable success – the Poole Council case which accounts for a full 50 per cent of the complaints it has upheld over the

[99] McIntyre n(79) 5.

last decade – was one in which the family was subsequently notified by the Council that they had been subject to surveillance.[100]

By providing for a right to notification, fundamental rights to privacy are subject to more stringent oversight and the right of individuals to seek remedies is strengthened.

d. Reclassification of CSPs

The limited rights of individuals are reinforced by the role played by CSPs and the fact that these companies are not bound by the requirements of the human rights instruments. In their role as generators of vast pools of information, CSPs have shifted from private actors to bodies fulfilling a public duty. Investigative and surveillance functions typically fall to public authorities. CSPs are increasingly being asked to perform functions related to these core law enforcement tasks. Historically, the private and public sectors were divided into two separate spheres with distinct areas of competence. The interplay between these two spheres was subject to legislation. In the case of data retention, CSPs could choose what data to retain and for how long, and access to this data could only be granted to law enforcement agencies following proper authorisation procedures.[101] As illustrated above, the development of the data retention regime placed additional obligations on CSPs in terms of retention, requiring the data to be retained for longer periods. As technological capabilities increased, the needs of CSPs to retain data for their own purposes began to diminish while the needs of law enforcement agencies to compel this retention to ensure further access increased. This has led to divergence in the

[100]JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age* (2011) < https://2bquk8cdew6192tsu41lay8t-wpengine.netdna-ssl.com/wp-content/uploads/2015/01/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf> accessed 25 Nov 2015, 139.
[101] These procedures for access were set out in the Regulation of Investigatory Powers Act 2000.

aims of the two parties, with CSPs being compelled to retain data that they no longer require simply to facilitate law enforcement goals.

Despite this, in fulfilling the statutorily mandated functions of retention, CSPs are still regarded as private actors, directly impacting on privacy by allowing intrusive measures to be undertaken without the subsequent protections that would be required if the process were performed by a public authority.[102] In recasting CSPs as public authorities, they could then be held accountable through mechanisms such as public oversight and judicial review.[103] A public authority would be bound to the protections guaranteed in the Human Rights Act 1998. Specifically, Section 6 HRA states that 'It is unlawful for a public authority to act in a way which is incompatible with a convention right'. However, there are exceptions to this provision; Section 6(3)(b) provides that a 'public authority' can include 'any person certain of whose functions are functions of a public nature', and section (6)(5) notes that, 'in relation to a particular act, a person is not a public authority by virtue of only subsection 3(b) if the nature of the act is private'. As a result, any person or body whose functions are of a public nature can be considered a public authority, other than in relations to those particular acts which are of a private nature.

It is argued that following these provisions, the role of the CSPs in retaining data should be classed as a 'function of a public nature' for the purposes of the HRA 1998. This argument is based on judicial precedent which holds that a private actor can be classed as 'performing a function of a public nature'.[104] This precedent establishes several criteria

[102] For further discussion on why to reclassify CSPs as public actors in this role see the author's article: Allison M Holmes, 'Private Actor or Public Authority? How the status of communications service providers affects human rights' (2017) 22 (1) Comm L 21.
[103] TJ McIntyre, 'Child Abuse images and Cleanfeeds: Assessing Internet Blocking Systems' in Brown (ed) *Research Handbook on Governance of the Internet* (Edward Elgar, 2013) 291.
[104] *Poplar Housing Association Ltd v Donoghue* (2001) 4 All ER 604; *Parochial Church Council of the Parish of Aston Cantlow, etc. v Wallbank* [2004] UKHL 37; *YL v Birmingham City Council* [2007] UKHL

to determine whether a private actor is fulfilling this public role, including: whether its actions are governed by statutory authority or contractual arrangements; whether there is an element of public funding; whether the body is acting in its own commercial interest; and whether there is a public interest in performing the function in question. CSPs retaining data fulfil these criteria.

First, CSPs are performing a duty which is imposed on them by statutory authority. As discussed in the foregoing analysis, they are required to retain data if placed under notice. The notice dictates who must retain the data, which services it must be retained for, how long it is retained for, and additional requirements or restrictions pertaining to the data.[105] While there is an element of consultation with CSPs before they are placed under a notice,[106] the requirement can be waived.[107] Further, the consultation does not require that CSPs' input or objections be taken into account nor do they have the ability to effectively challenge a notice, regardless of any potential costs or hardships it might place on them as a private company. CSPs are under a statutory duty to comply and a failure to comply with these requirements is enforceable through civil proceedings by the Secretary of State for an injunction or for the specific performance of a statutory duty under s 45 of the Court of Session Act 1988[108] or for any other appropriate relief.

Further, there is an element of public funding to the retention obligations placed on CSPs. CSPs are entitled to an appropriate contribution in respect of the costs incurred in complying with a notice.[109] It is recognised that different levels of contributions will be

27; *R (Weaver) v London and Quadrant Housing Trust* [2009] EWCA Civ 587; *Barr & Ors v Biffa Waste Services Ltd (No 3)* [2011] EWHC 1003;
[105] Home Office, *Retention of Communications Data* (Code of Practice, 2014) at para 3.3.
[106] *Ibid* para 3.9.
[107] *Ibid* para 3.13.
[108] Court of Session Act 1988 s 45(b) states that the Court may, on application by summary petition, order the specific performance of any statutory duty.
[109] IPA ss 249(1) & (2).

made but the appropriate contribution must never be nil.[110] This element of subsidy recognises that the notice imposes additional costs, particularly for CSPs who must employ staff specifically to manage compliance with the requirements of the notice. Neither the creation of these databases nor the hiring of additional staff to facilitate the retention of communications data for policing and intelligence purposes represents a profitable function for the company. Indeed, based on the precedent which forms the basis of the definition for 'functional public authorities', this element of public funding is indicative that the CSP is performing a 'function of a public nature'.

In addition, it is arguable that the CSP could be said to be acting in its own commercial interest in retaining the data. The value of the data to the company, due to development in technology and altered commercial models has decreased. For example, algorithmic processing of the data allows for quicker interpretation and decreased necessary retention period for processes like targeted advertising. Overall usage and call logs have diminished as the traditional method for paying for services; bundle payments and unlimited data arrangements are now the norm, making is unnecessary to retain specific details of usage and calls. The costs discussed above regarding the implementation measures of the notice similarly decrease the commercial value to the company. This does not however mean that no types of data retention are of value to the company; but rather the categories of data which they are required to retain to facilitate law enforcement are not necessarily those they would store for business purposes. This was acknowledged in the development of the data retention instruments. For example, Lord West noted the problem in his parliamentary contribution to the Investigatory Powers Bill:

[110] IPA s 249(6).

> I was made aware that changes to communications technology meant that a record of communications information would no longer be held by communications service providers and that technology was changing the types of data that were available. This information was held purely as it was needed for the companies' billing procedures – that is why they kept it - and, as such was available for use by properly authorised state officials, in particular for prosecution of 'serious crime' and terrorism cases. New technologies and methods of communication meant that firms were beginning to, and going to, charge differently.[111]

If the data which they are statutorily required to retain does not possess a commercial value, the question is what function are they fulfilling in retaining it? The argument is that they are fulfilling a public function primarily in the public interest in retaining the data. This is clear from the value of the data to law enforcement over the commercial value. If left to their own devices, the companies would not continue to retain the data at this level. This would thereby diminish the available data pools for law enforcement, as fact that has been frequently noted by the Government. 'Given the essential role communications data plays in assisting law enforcement agencies in protecting our citizens and bringing offenders to justice, the Government has for some years sought to ensure that it is retained and made available to appropriate public bodies lawfully, consistently, and efficiently'.[112] If the above criteria are satisfied, then the argument can be made to classify CSPs as performing a public function. As such, individuals whose privacy had been infringed by the actions of these companies would be able to challenge the procedures and better exercise their rights.

[111] HL Debates vol 759, cols 27-34, 26 Jan 2015.
[112] Explanatory Memorandum to the Data Retention (EC Directive) Regulations 2009, 3.

V. Concluding Remarks

This thesis has established that the current legal and policy frameworks governing the retention of, access to, and analysis of communications data by law enforcement represent a violation of privacy. This violation is not minimised or offset by the current oversight regime. Amendments to these legal and policy frameworks are necessary to ensure that an appropriate balance can be struck between privacy rights and the criminal law enforcement objectives of the State. As such, the thesis offers a prescriptive framework to correct the shortcomings of the current regime in a manner that better protects privacy. Privacy in this thesis has been conceptualised to take into account the significant normative changes which have resulted from the development of communicative technologies. As such, this conceptualisation of privacy, along with the analysis of how it can be applied to various data types, provides an avenue for further research into the use of technology by law enforcement.

Due to lack of resources and demands for greater efficiency, there is increasingly a drive toward the incorporation of technological tools into the policing process. These tools are based on various types of data, much of which do not fall easily into any communication/content distinction. Further, it is not necessarily possible to distinguish between what is personal and sensitive information and what is innocuous data. The inability to clearly or accurately classify data may lead to data being utilised in a manner inconsistent with the fundamental rights of individuals. This is particularly true as the generation of data is now lending itself increasingly toward algorithmic tools which are gaining acceptance in the policing process. The significance of these technologies and their normative implications remain unaddressed in legal and policy frameworks, but it is necessary to consider these issues and how to best address them before incorporating

them into instruments which can impact on individuals' fundamental rights. The issues raised in this thesis, regarding the changes in informational norms, can relate to the data incorporated into these systems. Future research can build on the findings herein to identify ways to ensure that legal and policy regimes better reflect the changes in norms associated with the use of new technologies by law enforcement in a manner that guarantees fundamental rights.

BIBLIOGRAPHY

Akedeniz Y Taylor N & Walker C, 'Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State Surveillance in the age of information and rights' (2001) Feb Crim LR 73.

Allen A, *Uneasy Access* (Rowman & Littlefield 1998).

Alvesson M, 'Beyond Neopositivists, Romantics, and Localists: A Reflexive Approach to Interviews in Organizational Research' (2005) 28(1) Academy of Management R 13.

Anderson C, 'The End of Theory: The Data Deluge Makes the Scientific Method Obsolete' *Wired* (Science 23 June 2008) <https://www.wired.com/2008/06/pb-theory/> accessed 19 Jan 2017.

Anderson D, *A Question of Trust: Report of the Investigatory Powers Review* (Stationary Office 2015).

Aronson J Cole S, 'Science and the Death Penalty: DNA, Innocence, and the Debate over Capital Punishment in the United States' (2009) 34(3) Law and Social Inq 603.

Austin L, 'Technological Tattletales and Constitutional Black Holes: Communications Intermediaries and Constitutional Constraints' (2016) 17 Theoretical Inq L 451.

Bacon F, *The Instauratio magna Part 2: Novum organum and Associated Texts* (Rees & Wakely (eds), Clarendon Press 2004).

Balmer A, 'Telling Tales: some episodes from the multiple lives of the polygraph machine' in Cloatre and Pickersgill (eds) *Knowledge, Technology and Law* (Routledge 2014).

Bellia P, 'Designing Surveillance Law' (2011) 43 Ariz St L J 293.

Bentham J, *Theory of Legislation* (Vol 1, Weeks Jordan & Co 1840).

Benzanson R, 'The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990' 80 Cal L R 5 1133.

Berry R, 'Updating our investigatory powers matters for day-to-day crime too' (*The Telegraph* 17 Oct 2016) <http://www.telegraph.co.uk/news/2016/10/17/updating-our-investigatory-powers-matters-for-day-to-day-crime-t/> accessed 4 Feb 2017.

Bigo D, 'Globalized (in)security: the Field and the Ban-opticon' in Bigo and Tsoukala (eds) *Terror, Insecurity, and Liberty: Illiberal Practices of Liberal Regimes after 9/11* (Routledge 2008).

- Bigo D Carrera S et al, 'National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU Law' (2013) European Parliament DG for Internal Policies PE 493.032.

Bijker W and Pinch T, 'The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other' in Bijker Hughes and Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012).

- Bijker W, ‘The Social Construction of Bakelite: Toward a Theory of Invention’ in Bijker Hughes and Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012).

Bingham T, ‘Report of the Interception of Communications Commissioner’ (1992).

Bloustein E, ‘Privacy as an aspect of Human Dignity: An Answer to Dean Prosser’ (1964) 39 NYU L R 926.

Bogard W, ‘Surveillance assemblages and lines of Flight’ in Lyon (ed) *Theorizing Surveillance: The Panopticon and Beyond* (Willan Publishing 2006).

Bok S, *Secrets: On the Ethics of Concealment and Revelation* (Pantheon 1983).

Bossewitch J and Sinnreich A, ‘The end of forgetting: strategic agency beyond the panopticon’ (2012) 15(2) New Media & Society 224.

Bowden C, ‘CCTV for inside your head: blanket traffic data retention and the emergency anti-terrorism legislation’ (2002) 8(2) Comp & Telecom L R 21.

Bowling B Marks A and Murphy C, 'Crime Control Technologies: Towards an Analytical Framework and Research Agenda' 60 in Brownsword and Yeung (eds), *Regulating Technologies* (Hart Publishing 2008).

boyd d and Crawford K, ‘Critical Questions for Big Data’ (2012) 15 Information, Communication, and Society 663.

Brighenti A, ‘Democracy and its visibilities’ in Haggerty and Samatas (eds) *Surveillance and Democracy* (Routledge 2010).

Brown I, 'Communications Data Retention in an Evolving Internet' (2010) 19(2) International Journal of Law and Information Technology.

- Brown I and Korff D, 'Combined Papers No 1 & 2: technology development and its effect on privacy and law enforcement' (FIPR 2004).

Brownsword R and Yeung K, 'Regulating Technologies: Tools, Targets, and Thematics' in Brownsword and Yeung (eds) *Regulating Technologies* (Hart Publishing 2008).

- 'Code, Control, and choice: Why east is east and west is west' (2005) 25 Legal Studies 1.

- 'So What Does the World Need Now? Reflections on Regulating Technologies' 27 in Brownsword and Yeung (eds), *Regulating Technologies* (Hart Publishing 2008).

Bryman A, *Social Research Methods* (Oxford University Press 2012).

Burnton S, *Report of the Interception of Communications Commissioner* (2016, HC 297).

Busch L, 'A Dozen Ways to Get Lost in Translation: Inherent Challenges in Large-Scale Data Sets' (2014) 8 Intl J of Comm 1727.

Callon M, 'Society in the Making: The Study of Technology as a Tool for Sociological Analysis' in Bijker Hughes and Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012).

Caluya G, 'The post-panoptic society? Reassessing Foucault in surveillance studies' (2010) 16(5) Social Identities 621.

Campbell D, ‘Assessing the impact of Planned social change’ (1979) 2 Eval & Prog Planning 67.

Cannatacci J, ‘Report of the Special Rapporteur on the Right to Privacy’ (UN General Assembly 30 Aug 2016) A/71/368.

Castells M, ‘An Introduction to the Information Age’ in Webster (ed) *The Information Society Reader* (Routledge 2004).

- *Communication Power* (Oxford University Press 2013).

Cate F, *Privacy in the Information Age* (Brookings Institution Press 1997).

CJEU, Opinion 1/15 on the Draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, Opinion of the Court (Grand Chamber), 26 July 2017.

Clarke R, ‘Information Technology and Dataveillance’ (1988) 31(5) Comm of the ACM 498.

Cloatre E Pickersgill M, ‘Introduction’ in Cloatre and Pickersgill (eds) *Knowledge, Technology and Law* (Routledge 2014).

Cobain I and Haddou L, ‘”Independent” court scrutinising MI5 is located inside Home Office’ (*The Guardian* 5 Mar 2014) < https://www.theguardian.com/politics/2014/mar/05/independence-ipt-court-mi5-mi6-home-office-secrecy-clegg-miliband> accessed 11 Nov 2017.

Cohen J, ‘Examined Lives: Informational Privacy and the Subject as Object’ (1999) 52 Stan L R 1373.

- *Configuring the Networked Self* (Yale Uni Press 2012).
- 'The Regulatory State in the Information Age' (2016) 17 Theoretical Inq L 369.

Constant E, 'The Social Locus of Technological Practice: Community, System, or Organization?' in Wiebe Bijker, Thomas P Hughes, and Trevor Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012).

Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' CON (1985) 108

- 'Study on the Human Rights Dimensions of Automated Data Processing Techniques (in particular Algorithms) and Possible Regulatory Implications' MSI-Net (2016) 06 rev 3 FINAL 13
- 'Recommendation of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries' CM/Rec (2018).

Craven J B, 'Personhood: The Right to be Let Alone' (1976) 15 Duke L J 699.

Crawford K, 'The Hidden Biases in Big Data' *Harvard Business Review* (1 April 2013) < https://hbr.org/2013/04/the-hidden-biases-in-big-data> accessed 15 June 2017.

- Schultz J, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) Boston C L R 93.
- 'Critiquing Big Data: Politics, Ethics, Epistemology' (2014) 8 Intl J of Comm 1663.

Dash S Schwartz R & Knowlton R, *The Eavesdroppers* (De Capo Press 1971).

Daskal J, ‘The Un-Territoriality of Data’ (2015-2016) 125 Yale L J 326.

Deleuze G & Guattari F, *A Thousand Plateaus: Capitalism and Schizophrenia* (U of Minn Press 1987).

Dewey J, *Logic: The Theory of Inquiry* (Holt Reinhart and Winston 1938).

- ‘Ethics’ (1908) in Boydston (ed) *The Middle Works of John Dewey 1899-1924* (Southern Illinois University Press 1978).

Edwards L, ‘Privacy and Data Protection Online: The Laws Don’t Work?’ in Edwards and Waeld (eds) *Law and the Internet* (Hart 2009).

Eggenschwiler J, ‘Accountability challenges confronting cyberspace governance’ (2017) 6 Internet Policy Review 3.

Elkin-Koren N and Haber E, ‘Governance by Proxy: Cyber Challenges to Civil Liberties’ (2016) 82 Brooklyn L R 105.

Elliot M, ‘Through the Looking Glass? Ouster Clauses, Statutory Interpretation, and the British Constitution’ (2018) University of Cambridge Legal Studies Research Paper 4/2018.

Epstein, R ‘The Legal Regulation of Genetic Discrimination: Old Responses to New Technology’ (1994) 74 Boston U L R 1.

Ericson R and Haggerty K, *Policing the Risk Society* (Clarendon Press 1997).

European Commission, *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)* (18.4.2011, COM (2011) 225 final, 2011).

- S*taff working document - Annex to 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 - Extended impact assessment* (0438, 2005) 1131.

European Union Agency for Fundamental Rights, *Fundamental Rights Report* (FRA 2016).

- 'Surveillance by Intelligence services: fundamental rights, safeguards, and remedies' (2017) Vol 2.

Europol, 'Are you sharing the same IP address as a criminal? Law enforcement call for the end of carrier grade nat (CGN) to increase accountability online' (Europol Press Office) < https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online> accessed 18 Oct 2017.

Explanatory Memorandum to the Data Retention (EC Directive) Regulations 2007.

Explanatory Memorandum to the Data Retention (EC Directive) Regulations 2009.

Explanatory Notes to the Counter-Terrorism and Security Bill 2014.

Explanatory Notes to the Counter-Terrorism and Security Act 2015.

Explanatory Notes to the Data Retention and Investigatory Powers Act 2015.

Explanatory Notes to the Data Protection Act 2018.

Explanatory Notes to the Investigatory Powers Act 2016.

Faulkner A Lange J & Lawless C, 'Introduction: Material Worlds: Intersections of Law, Science, Technology and Society' (2012) 39(1) J of L and Soc 1.

Fisher C, *America Calling: A Social History of the Telephone from 1940* (University of California Press 1994).

Flear M Pickersgill M, 'Regulatory or regulating publics? The European Union's Regulation of Emerging Health Technologies and Citizen Participation' (2013) 21 Medical L Rev 39.

Foucault M, *Discipline and Punish* (Alan Sheridan tr, Penguin 1991).

Fox-Brewster T, 'Forget About Backdoors, This is the Data WhatsApp actually Hands to Cops' (*Forbes* 22 June 2017) <https://www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/#64dda5141030> accessed 27 July 2018.

Fried C, 'Privacy' (1967-1968) Yale L J 475.

Freund P, 'Privacy: One Concept or Many' in Pennock and Chapman (eds) *Nomos XIII: Privacy* (1971).

Froomkin A M, 'The Death of Privacy?' (2000) 52 Stanford L R 1462.

Fulford A, 'Investigatory Powers Commissioner's Office Letter response to Privacy International, Liberty, Big Brother Watch, and the Open Rights Group' (13 Oct 2017) <https://ipco.org.uk/docs/2017%2010%2013%20IP%20Commissioner%20response%20to%20Privacy%20International%20et%20al.pdf> accessed 19 Oct 2017.

- 'Investigatory Powers Commissioner's Office Press Release on the Appointment of Judicial Commissioners' (18 Oct 2017) < https://www.judiciary.gov.uk/wp-content/uploads/2017/10/jc-announcement-13-new-commissioners-oct2017.pdf> accessed 19 Oct 2017.

Gavison R, 'Privacy and the Limits of Law (1980) 89 Yale L J 421.

Gidda M, 'Edward Snowden and the NSA files – timeline' *The Guardian* (London, 21 Aug 2013) <https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline> accessed 11 Oct 2014.

Gillespie T, 'The Relevance of Algorithms' in Gillespie Boczkowski and Foot (eds) *Media Technologies: Essays on Communication, Materiality, and Society* (MIT Press 2014).

Goffman E, *The Presentation of Self in Everyday Life* (Doubleday 1959).

Golan T, *Laws of Men and Laws of Nature* (Harvard Uni Press 2004).

Goold B, 'Liberty and others v The United Kingdom: a new chance for another missed opportunity' (2009) P L 5.

Graham C, Liverpool John Moore's Roscoe Lecture (12 Jan 2015).

Greenberg, A 'It's been 20 years since this man declared cyberspace independence' *Wired* (2 Aug 2016) <https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/> accessed 15 Sept 2016.

Greenwald G, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily', *The Guardian* (6 June 2013)

<http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> accessed 11 Oct 2014.

- *No Place to Hide*, (Penguin 2014).

Gross H, 'The Concept of Privacy' (1967) 42 NYU L Rev 34.

Gutwirth S, *Privacy and the Information* Age (Raf Casert 2002).

Haggerty K & Ericson R, 'The surveillant assemblage' (2000) 51(4) Brit J of Sociology 606.

- Haggerty K, 'Tear down the walls: on demolishing the Panopticon' in Lyon (ed), *Theorizing Surveillance: The Panopticon and Beyond* (Willan Publishing 2006).

Haraway D, *Simians, Cyborgs, and Women: The Reinvention of Nature* (Routledge 1991).

HC Debates vol 944 cols 760-1W, 23rd Feb 1978.

- HC Debates vol 947, cols 476-7 W, 13 April 1978.
- HC Debates col 162, 12 March 1985.
- HC Debates col 163, March 1985.
- HC Debates col 705, 15 July 2014.
- HC Debates vol 589, col 214, 2 Dec 2014.
- HC Debates vol 587 col 970, 4 November 2015.
- HC Debates vol 607, col 240 14 April 2016.

Heilbroner R, 'Do Machines Make History' in Johnson and Wetmore (eds), *Technology and Society: Building our Sociotechnical Future* (MIT Press 2008).

Hill M, Independent Reviewer of Terrorism Legislation; 'Rights vs Security: the challenge Engaged' (24 Oct 2017) Tom Sargant Memorial Lecture for JUSTICE.

HL Debates col 373, 20 March 2008.

- HL Debates vol 759, cols 27-34, 26 Jan 2015.
- HL Debates vol 788, col 1710, 1 February 2018.

HMCIC, *State of Policing: The Annual Assessment of Policing in England and Wales* (2017) <https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/state-of-policing-2017-2.pdf> accessed 8 May 2018.

Holmes A, 'Private Actor or Public Authority? How the status of communications service providers affects human rights' (2017) 22 (1) Comm L 21.

- 'Automated Investigations: The Role of the Request Filter in Communications Data Analysis' (2018) 2(2) J of Info Rights Practice & Policy.

Home Affairs Committee, *Policing for the Future* (HC 2017-19, 515-X).

Home Office, *Protecting the Public in a Changing Communications Environment* (Cmd 5668, 2009).

- *Acquisition and Disclosure of Communications Data Code of Practice* (March 2015)
- *Communications Data DRAFT Code of Practice* (June 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/724394/CCS207_CCS0618947544-

001_Home_Office_Publication_of_Codes_CLIENT_PRINTIN....pdf> accessed 7 July 2018.

- *Draft Communications Data Bill Written Evidence* (2012-13) 242.
- *Government Consultation on the Investigatory Power Act* (November 2017).
- 'Impact Assessment: Domestic Right of Appeal for the IPT' (7 July 2016) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/538312/domestic-right-of-appeal-from-the-Investigatory-Powers-Tribunal.pdf>.
- *Investigatory Powers Tribunal Consultation: Updated Rules* (September 2017).
- *Operational Case for Bulk Powers* (2016) < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf> accessed 15 Dec 2016.
- *Operational Case for the Retention of Internet Connection Records* (4 November 2015).
- *Regulation of Investigatory Powers Act Consultation: Acquisition and Disclosure of Communications Data and Retention of Communications Data Codes of Practice* (2014).
- *Retention of Communications Data Code of Practice* (9 December 2014).

Horton M, *The Closing of the Net* (Polity Press 2016).

House of Commons Justice Committee, 'The functions, powers and resources of the Information Commissioner' (9th Report of Session 2012-13 edn House of Commons 2013).

- 'Investigatory Powers Bill: Technology Issues' (HC573 2015).

House of Lords and House of Commons 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* (The Stationary Office Sixteenth Report, 2002-03) HC 1272.

- *Surveillance: Citizens and the State* (2009, HL 18).

Hughes T, 'Technological Momentum' in Johnson and Wetmore (eds), *Technology and Society: Building our Sociotechnical Future* (MIT Press 2008).

- 'The Evolution of Large Technological Systems' in Bijker Hughes, and Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012).

Information Commissioner's Office, 'Draft Data sharing code of practice' (2018) < https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf>.

Investigatory Powers Commissioner's Office, 'Who we are', (*Investigatory Powers Commissioner's Office* 2018) < https://www.ipco.org.uk/default.aspx?mid=14.12> accessed 15 Jan 2018.

Investigatory Powers Tribunal, *Annual Reports 2011-2015* (2016) < http://ipt-uk.com/docs/IPT%20Report%202011%20-%202015.pdf>

- *Report of the Investigatory Powers Tribunal*, (2016) <http://ipt-uk.com/docs/IPT%20Report%202011%20-%202015.pdf>.
- 'Appointment Process' (*Investigatory Powers Tribunal*, 5 Jul 2016) <*https*://www.ipt-uk.com/content.asp?id=21>.

Inness J, *Privacy, Intimacy, and Isolation* (Oxford University Press 1996).

Jasanoff S, *Science at the Bar: Law, Science, and Technology in America* (Harvard Uni Press 1995).

- 'The idiom of co-production' in Jasanoff (ed) *States of Knowledge: The co-production of science and social order* (Routledge 2004).
- 'Ordering knowledge, ordering society' in Jasanoff (ed) *States of Knowledge: The co-production of science and social order* (Routledge 2004).
- 'Afterword' in Jasanoff (ed) *States of Knowledge: The co-production of science and social order* (Routledge 2004).
- 'Just Evidence: The Limits of Science in the Legal Process' (2006) 34 J L Med & Ethics 328.

Jasserand C, 'Law Enforcement access to personal data originally collected by private parties: Missing Data subjects' safeguards in directive 2016/680?' (2018) 34 Comp L & Sec Rev 154.

Johnson D and Post D, 'Law and Border: The Rise of Law in Cyberspace' (1996) 48 Stanford L R 1367.

Joint Committee, *Draft Communications Data Bill* (2012-13, HL 79, HC 479).

- Written Evidence for the Investigatory Powers Bill Law Enforcement Submission.
- Written Evidence for the Investigatory Powers Bill National Crime Agency < http://www.nationalcrimeagency.gov.uk/publications/673-written-evidence-annexes-a-d/file>.

Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (Communication) 2017 JOIN 0450 final 14.

Jourard S, 'Some Psychological Aspects of Privacy' (1966) 31 Law & Contemp Prob 307.

JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age* (2011) < https://2bquk8cdew6192tsu41lay8t-wpengine.netdna-ssl.com/wp-content/uploads/2015/01/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf> accessed 25 Nov 2015.

- *To "Neither Confirm Nor Deny": Assessing the Response and its Impact on Access to Justice* (2017).

Kalven H, 'Privacy in Tort Law – Were Warren and Brandies Wrong?' [1966] 31 Law & Contemp Prob 326.

Kaplan D, *Readings in the Philosophy of Technology* (Rowman & Little 2004).

Karst K, 'The Files: Legal Controls over the Accuracy and Accessibility of Stored Personal Data' (1966) 31 Law & Contemp Prob 342.

Kelly K, *What Technology Wants* (Penguin Books 2010).

Kerr O, 'The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution' (2004) 102 Michigan L R 801.

Kesan J and Shah R, 'Deconstructing Code' (2003-2004) 6 Yale L J 277.

Kim N and Telman J, 'Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent' (2015) 80 Mo L R 723.

King J and Richards N, 'What's Up with Big Data Ethics' *Forbes* (28 March 2014) < https://www.forbes.com/sites/oreillymedia/2014/03/28/whats-up-with-big-data-ethics/#e47520435913> accessed 11 Sept 2018.

Kirby M, 'New Frontier: Regulating Technology by Law and 'Code'' in Brownsword and Yeung (eds), *Regulating Technologies* (Hart Publishing 2008).

Kirkpatrick D, *The Facebook Effect: The Real Inside Story of Mark Zuckerberg and the World's Fastest Growing Company* (Virgin Books 2011).

Knorr-Cetina K, *Epistemic Cultures: How the Sciences Make Knowledge* (Harvard Uni Press 1999).

Kohl U, *Jurisdiction and the Internet* (Cambridge University Press 2007).

Koops BJ, 'Criteria for Normative Technology: The Acceptability of 'Code as Law' in light of Democratic and Constitutional Values' in Brownsword and Yeung (eds) *Regulating Technologies: Legal Futures, Regulatory Frames, and Technological Fixes* (Hart 2008).

- Leenes R, '"Code" and the Slow Erosion of Privacy' (2005) 12(1) Mich Telecom & Tech L R 335.

Korff et al, 'Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes' (Legal Studies Research Paper Series, University of Cambridge Paper No 16/2017) March 2017.

Kranzberg M, ‘Technology and History: “Kranzberg’s Laws”’ (1986) 27(3) Technology and Culture 544.

La Rue F, ‘Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression’ (UN 2013) A/HRD/23/40 82.

Law in Action, Interview with Justice Burnton, President of the Investigatory Powers Tribunal, BBC Radio 4 (7 Nov 2013).

Law J, ‘Technology and Heterogeneous Engineering: The Case of Portuguese Expansion’ in Bijker Hughes & Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012).

Lessig L, ‘The Law of the Horse: What Cyberlaw Might Teach’ (1999) Harvard L R 531

- *Code and Other Laws of Cyberspace: Version 2.0* (Basic Books 2006).
- *Code 2.0* (2 edn, Createspace 2009).

Liberty, R*esponse to the Home Office Consultation on the Acquisition and Disclosure of Communications Data and the Retention of Communications Data Codes of Practice* (Liberty Jan 2015).

- *Response to the Government’s consultation on the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data* (18 Jan 2018) < https://www.libertyhumanrights.org.uk/sites/default/files/2018.01.18%20liberty%20consultation%20response%20FINAL.pdf> accessed 4 Feb 2018.

Lyon D, 'The new surveillance: Electronic technologies and the maximum security society' (1992) 18 Crime, Law, and Social Change 159.

- 'A Sociology of Information' in Calhoun Rojek and Turner (eds) *The SAGE Handbook of Sociology* (SAGE 2005).

MacAskill E, Borger J, Hopkins N, Davies N, & Ball J, '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> accessed 15 June 2014.

MacKenzie D, 'Missile Accuracy: A Case Study in the Social Processes of Technological Change' in Bijker Hughes and Pinch (eds), *The Social Construction of Technological Systems* (MIT Press 2012).

Mackey A Schoen S and Cohn C, 'Unreliable Informants: IP Addresses, Digital Tips, and Police Raids: How Police and Courts are Misusing Unreliable IP address Information and What they can do' (EFF 2016).

Maisog M, 'Making the Case against Data Localization in China' (IAPP 20 April 2015) < https://iapp.org/news/a/making-the-case-against-data-localization-in-china/> accessed 11 Nov 2016.

Mansell R, *Draft Communications Data Bill Written Evidence* (2012-13).

Marsden C and Brown I, *Regulating Code* (MIT Press 2013).

Marwick A & boyd d, 'Networked privacy: How teenagers negotiate context in social media' (2014) 16(7) New Media & Society 1051.

Marx G, 'The Declining Significance of Traditional Borders (and the Appearance of New Borders) in an Age of High Technology' in Droege (ed) *Intelligent Environments* (Elsevier Science 1997) 484.

- 'Murky Conceptual Waters: The Public and the Private' (2001) 3 Ethics & Info Tech 157.
- 'Some Conceptual Issues in the Study of Borders and Surveillance' 23 in Zuriek and Salter (eds) *What Goes There? Global Policing and Surveillance* (Willan 2005).
- 'Coming to terms: the kaleidoscope of privacy and surveillance' 32 in Roessler and Mokrosinska (eds) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015).
- 'Surveillance Studies' in Wright (ed) *International Encyclopaedia of the Social & Behavioural Sciences* (2 edn, Elsevier 2015).

Marx K and Engels F, *Collected Works* (Vol 5 Lawrence & Wishart 2010).

Marx L and Roe Smith M, *Does Technology Drive History?: The Dilemma of Technological Determinism* (MIT Press 1994).

May A, *Annual Report of the Interception of Communications Commissioner* (HC1184, 2013).

McIntyre TJ, 'Intermediaries, Invisibility, and the Rule of Law' (March 2008) BILETA Conference Paper.

- and Scott C, ‘Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility’ in Brownsword and Yeung (eds) *Regulating Technologies* (Hart 2008) 109.
- ‘Child Abuse images and Cleanfeeds: Assessing Internet Blocking Systems’ in Brown (ed) *Research Handbook on Governance of the Internet* (Edward Elgar 2013) 277 – 308.
- ‘Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective’ in Scheinin Krunke and Askenova (eds) *Judges as Guardians of Constitutionalism and Human Rights* (Edward Elgar 2016).

McClosky HJ, ‘Privacy and the Right to Privacy’ (1980) 55 Philosophy 37.

Michaels J, ‘All the President’s Spies: Private-Public Intelligence Partnerships in the War on Terror’ (2008) 96 Cal L R 901.

Mill J S, *On Liberty* (Andrews UK Ltd 1890).

Miller V, *The Crisis of Presence in Contemporary Culture* (Sage 2016).

Monahan T, ‘Questioning Surveillance and Security’ in Johnson and Wetmore (eds), *Technology and Society: Building our Sociotechnical Future* (MIT Press 2008).

Morozov E, *To Save Everything Click Here* (Penguin 2013).

Nissenbaum H, *Privacy in Context* (Stanford University Press 2010).

- ‘Respect for Context as a benchmark for privacy online: what it is and isn’t’ 286 in Roessler and Mokrosinska (eds) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015).

- '"Respect for Context": Fulfilling the Promise of the White House Report' in Rotenberg Horowitz and Scott (eds) *Privacy in the Modern Age* (The New Press 2015).

Norris C and Armstrong G, *The Maximum Surveillance Society* (1999 Berg).

O'Brien D M, *Privacy, Law and Public Policy* (Praeger 1979).

O'Donnell G, 'The Quality of Democracy: Why the Rule of Law Matters' (2004) 15 J of Democracy 4, 31.

OFCOM, *Communications Market Report 2016* (4 Aug 2016) < https://www.ofcom.org.uk/__data/assets/pdf_file/0024/26826/cmr_uk_2016.pdf> accessed 12 Jan 2017.

- *Report on the Implications of Carrier Grade Network Address Translators* (2013 MC/159).

Office of Communications Data Authorisations, 'Authorising Officer Candidate Information Pack' (18 May 2018) < file:///C:/Users/amh56/Downloads/676313.pdf> accessed 6 June 2018.

Oxford Pro Bono Publico, 'Legal Opinion on Intercept Communications' (University of Oxford 2006).

Padmanabhan R Dhamdhere A et al, 'Reasons Dynamic Addresses Change' (ACM-IMC, Santa Monica, November 2016).

Parker R, 'A Definition of Privacy' (1974) 27 Rutgers L R 280.

Pickering A, *The Mangle of Practice: Time, Agency, and Science* (Uni of Chicago Press 1995).

Poitras L, *Citizenfour* (Praxis Films 2014).

Posner R, *The Economics of Justice* (Harvard University Press 1981).

- 'Our Domestic Intelligence Crisis' *The Washington Post* (Opinions 21 Dec 2005) <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html> accessed 17 Jan 2017.
- *Not a Suicide Pact: The Constitution in a Time of National Emergency* (Oxford University Press 2006).

Post R, 'The Social Foundations of Privacy: Community and Self in Common Law Tort' (1989) 77 Cal L R 980.

Poster M, *The Mode of Information: Poststructuralism and Social Context* (Chicago University Press 1990).

Prainsack B, 'Unchaining research: processes of dis/empowerment and the social study of criminal law and investigation' in Cloatre and Pickersgill (eds) *Knowledge, Technology and Law* (Routledge 2014).

Rachels J, 'Why Privacy is Important' (1975) 4(4) Phil & Pub Affairs 323.

Rauhofer J, 'Privacy and Surveillance: Legal and Socioeconomic Aspects of State Intrusion into Electronic Communications' in Edwards and Waelde (eds), *Law and the Internet* (Hart Publishing 2009).

- ‘The Retention of Communications Data in Europe and the UK’ in Edwards and Waelde (eds) *Law and the Internet* (Hart Publishing 2009).

Regan P, *Legislating Privacy* (University of North Caroline Press 1995).

‘Privacy and the common good: revisited’ 51 in Roessler and Mokrosinska (eds) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015).

Reidenberg J, ‘States and Internet Enforcement’ (2003-2004) 1 U Ottawa L & T J 213.

Reiman J, ‘Privacy, Intimacy, and Personhood’ (1976) 6(1) Phil & Pub Affairs 26.

- ‘Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future’ (1995) 11 (1) Santa Clara Comp & High Tech L J 42.

Richards N and King J, ‘Big Data Ethics’ (2014) 49 Wake Forest L R 393.

Ritzer G, ‘Control: Human and Nonhuman Robots’ in Johnson and Wetmore (eds), *Technology and Society: Building our Sociotechnical Future* (MIT Press 2008).

Roe Smith M, ‘Technological Determinism in American Culture’ in Marx and Roe Smith (eds) *Does Technology Drive History?: The Dilemma of Technological Determinism* (MIT Press 1994).

Roessler B, *The Value of Privacy* (Polity Press 2004).

- ‘Privacy and social interaction’ (2013) Phil & Social Criticism 779.

Rosen J, *The Unwanted Gaze: The Destruction of Privacy in America* (Vintage Books 2000).

Roulston K, 'Considering quality in qualitative interviewing' (2010) 10(2) Qualitative Research 206.

Rowland Kohl and Charlesworth, *Information Technology Law* (4th edn) (Routledge 2012).

Rozenshtein A, 'Surveillance Intermediaries' (2017) 70 Stanford L R 1.

Rubenfeld J, 'The Right of Privacy' (1988-1990) 102 Harv L Rev 737.

Sarewitz D, 'Pas de Trois: Science, Technology, and the Marketplace' in Johnson and Wetmore (eds), *Technology and Society: Building our Sociotechnical Future* (MIT Press 2008).

Sashina A, 'Russian Data Localization Law: commentary of the Ministry of Communications' (*Bird & Bird*, 28 Aug 2015) < https://www.twobirds.com/en/news/articles/2015/global/russian-data-localistation-law> accessed 11 Nov 2016.

Scanlon T, 'Thomson on Privacy' (1975) 4 Phil & Pub Affairs 315.

Schoeman F, 'Privacy: Philosophical Dimensions of the Literature' in Schoeman (ed) *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press 1984).

Schneier B, ‘Security Trade-Offs Are Subjective’ and ‘Technology Creates Security Imbalances’ in Johnson and Wetmore (eds), *Technology and Society: Building our Sociotechnical Future* (MIT Press 2008).

- *Data and Goliath* (WW Norton & Co 2015).

Schwartz P, ‘Privacy and Democracy in Cyberspace’ (1999) 52 Vand L R 1609.

Scott P, ‘Ouster clauses and national security: judicial review of the Investigatory Powers Tribunal’ (2017) P L 355.

Shils E, ‘Privacy: Its Constitution and Vicissitudes’ (1966) 31 L and Contemp Prob 281.

Siepp D, *The Right to Privacy in American History* (Harvard University Program on Information Resources Policy, 1978).

Silverman D, *Interpreting Qualitative Data: Methods for Analysing Talk, Text, and Interaction* (Sage 2001).

Simitis S, ‘Reviewing Privacy in an Information Society’ (1987) 135 U Pa L R 707.

Simmel A, ‘Privacy is not an Isolated Freedom’ in Pennock and Chapman (eds) *Nomos XIII* (1971).

Smutny Z, ‘Social informatics as a concept: Widening the discourse’ (2016) 5 Journal of Information Science 42, 681.

Solove D, ‘Reconstructing Electronic Surveillance Law’ (2004) 72 GW L R 1264.

- *Understanding Privacy* (Harvard University Press 2008).

- *Nothing to Hide: the False Tradeoff between Privacy and Security* (Yale University Press 2011).

Sommer P, *Draft Communications Data Bill Written Evidence* (2012-13) 526.

Star S L, 'Simplification in Scientific work: An example from neuroscience research' (1983) 13 Social Studies of Science 205.

Steeves V, 'Privacy, sociality, and the failure of regulation: lessons learned from young Canadians' online experiences' in Roessler and Mokrosinska (eds) *Social Dimensions of Privacy* (Cambridge U Press 2015).

Sunstein C, 'The Laws of Fear' (2002) Harvard LR 1119.

Taddeo M and Floridi L, 'The Moral Responsibilities of Online Service Providers' in Taddeo and Floridi (eds) *The Responsibilities of Online Service Providers* (Springer 2017).

Technical Advisory Board, *Annual Report* (2014-2015) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/477901/Technical_Advisory_Board_Annual_Report_2014-15.pdf> accessed 17 Dec 2017.

Thomson J, 'The Right to Privacy' (1975) 4 Phil & Pub Affairs 295.

Travis A and Norton-Taylor R, 'Private firm may track all email and calls' *The Guardian* (London 31 Dec 2008) https://www.theguardian.com/uk/2008/dec/31/privacy-civil-liberties accessed 2 Feb 2017.

- Wintour P, and MacAskill E, 'Theresa May unveils UK surveillance measures in wake of Snowden claims' *The Guardian* (4 Nov 2015) <https://www.theguardian.com/world/2015/nov/04/theresa-may-surveillance-measures-edward-snowden> accessed 20 Oct 2016.

Trevisani P, 'Brazil Lawmakers Remove Controversial Provision in Internet Bill' *Wall Street Journal* (Brasilia, 19 March 2014) < https://www.wsj.com/articles/SB10001424052702304026304579449730185773914> accessed 11 Nov 2016.

UNHCHR, *Guiding Principles on Business and Human Rights* (2011 HR/PUB.11.04).

UNHCHR and CoE, *The rule of law on the Internet and the wider Digital World* (2014).

Van Brakel R and De Hert P, 'Policing, surveillance and law in a pre-crime society: Understanding the consequence of technology based strategies' (2011) 20 J of Police Studies 163.

Van den Haag E, 'On Privacy' in Pennock and Chapman (eds) *Nomos XIII: Privacy* (1971).

Verbeek P-P, 'Moralising Morality: Design Ethics and Technological Mediation' (2006) 31(3) Science, Technology & Human Values 361.

Wacks R, *'Law Morality and the Private Domain* (Columbia University Press 2000).

Walker C, 'Data retention in the UK: Pragmatic and proportionate, or a step too far?' (2009) 25 Computer Law & Security Review 325.

Ward P, *The Data Retention and Investigatory Powers Bill* (House of Commons Library 14.7.2014, SN/HA/6934, 2014).

Warren C, *Handbook of Interview Research* (Sage Publications 2002).

Warren S and Brandeis L, 'The Right to Privacy' (1890-1891) 4 Harv L Rev 193.

Westin A, *Privacy and Freedom* (The Bodley Head 1967).

Wevell R, (Interview) Head of the IOCCO, Home Office (June 2016).

White L, *Medieval Technology and Social Change* (Oxford University Press 1966).

Whitley E and Hosein I, 'Policy discourse and data retention: The technology politics of surveillance in the United Kingdom' (2005) 29 Telecommunications Policy 857.

Winner L, *The Whale and the Reactor* (U of Chicago Press Books 1986).

Wittgenstein L, *Philosophical Investigations* (Blackwell Publishers 2001).

Woods A, 'Against Data Exceptionalism' (2016) 68 Stan L R 729.

Woolgar S, *Knowledge and Reflexivity: New Frontiers in the Sociology of Knowledge* (Sage 1988).

Wright D Friedewald M Gutwirth S and Bigo D, 'Sorting out Smart Surveillance' (2010) 26(4) Comp L & Sec Report.

Yeung K, ‘Hypernudge: Big Data as a mode of regulation by Design’ (2017) 20(1) Info, Comm, & Soc 118.

Zedner L, ‘Pre-crime and post criminology?’ (2007) 11(2) Theoretical Criminology 261.

Zittrain J, *The Future of the Internet* (Penguin Books 2008).

- ‘Perfect Enforcement on Tomorrow’s Internet’ in Brownsword and Yeung (eds) *Regulating Technologies* (Hart 2008).