FACULTY OF LAW

Lund University

Spencer Cameron Whiskard

Internet Surveillance Law in the UK and Article 8 'Right to Privacy'

International Human Rights Law

Graduate Thesis, Master of Laws Program

30 Higher Education Credits

Supervisor: Karol Nowak

Spring 2017

Contents

Abbreviations

Bulk Personal Datasets: BPD

Closed Circuit Television: CCTV

Communications Service Provider: CSP

Computer Misuse Act 1990: CMA

Crown Prosecution Service: CPS

Data Retention and Investigatory Powers Act 2014: DRIP

European Convention on Human Rights: ECHR

European Court of Human Rights ECtHR

European Court of Justice: ECJ

Equipment Interference: EI

European Union: EU

Global Positioning System: GPS

Her Majesty's Revenue and Customs: HMRC

Interception of Communications: IOC

Internet Protocol Address: IP

Internet Service Provider: ISP

Investigatory Powers Act 2016: IPA

Investigatory Powers Commission: IPC

Investigatory Powers Tribunal: IPT

Judicial Commissioners: JC

Member of Parliament: MP

National Health Service: NHS

Regulation of Investigatory Powers Act 2000: RIPA

Telecommunications Service Provider: TSP

Video Cassette Recorder: VHS

Research Question

Firstly, I wish to explore the idea of 'privacy' from a philosophical, practical and legal perspective through highlighting the concept's historically problematic relationship with laws and methods of state surveillance. Of key importance is showing how developing technologies and, in particular, the invention of the Internet has brought this controversial dichotomy to the forefront of legal, political and ethical discourse in 21st-century western society.

I will continue by taking a critical eye to the UK's most recent addition to its surveillance corpus; the Investigatory Powers Act 2016 (IPA 2016). The critique will be conducted in conjunction with the prevailing legal stances of the European Court of Human Rights (ECtHR) towards similar forms of surveillance legislation, proposed or enacted by others parties to the European Convention on Human Rights (ECHR) in line with Article 8 ECHR; the right to privacy. My critique will also draw upon relevant commentary from the discourse outlined above.

These investigations will contribute towards providing a tentative answer to the question of whether the IPA 2016 can be considered 'legal' under Article 8 ECHR, in accordance with ECtHR jurisprudence. Notwithstanding, I also wish to provide a response to the question of whether the ECtHR's position on Internet surveillance legislation, under Article 8 ECHR, can be considered 'right' or 'correct'. I will draw upon my previous findings on the nature of 'privacy' and also analyze the methods of reasoning employed by the court in order to inform my conclusion. Instead of trying to find a strict answer, as to whether they are indeed 'right' or 'wrong' in their stance (this is highly subjective), my idea with this question is simply to illuminate the fact that the ECtHR is, perhaps, not the best-equipped institution to deal with the highly complicated legal issues that come with such rapidly developing technology. I will determine whether there is any truth to this during the course of my thesis.

Thesis structure

Chapter 1 introduces some key concepts which will serve as the conceptual underpinning the thesis. It will also provide a brief history of surveillance, the purpose of which is to show how progressing technology can alter what is deemed as an acceptable practice. **Chapter 2** will introduce the Investigatory

Powers Act 2016 (IPA) and detail its salient provisions. It will close with a commentary on the nature of its provisions with reference to previous discussions. **Chapter 3** is about Article 8 ECHR and the court's assessment of surveillance cases that have been brought under the aforementioned Article. Through extrapolation, I will assess the legality of the IPA 2016 and then provide commentary on whether the ECtHR works within the parameters I have strived to highlight. **Chapter 4** will be the conclusion; it will round-up the thesis in its entirety, form tentative conclusions and end with some final remarks.

Research Methodology and Materials

'Privacy' is a highly amorphous concept; highly debated, frequently misunderstood and constantly evolving against an ever-changing political, sociological and technological environment. In order to critically assess contemporary laws that serve to protect or potentially infringe 'privacy', it is imperative to flesh out the meaning of the term as much as is reasonably practicable.

This is achievable by presenting the historical arguments that have persistently accompanied debates on whether the protection of privacy in the law should be strengthened in response to arguably *intrusive* state policies and application of new technologies. It is my desire that the sociological and philosophical ideas that underpin alternate viewpoints will organically emerge in the course of this exploration. I will utilize academic material to this effect.

Once the historical context has been established, this will serve as a useful springboard from which to explore the philosophical/social concepts of privacy in more depth. At this point we have a grasp of how privacy *has been* understood, but what are the opinions on how privacy *should be* understood? To provide some insight, I will observe the works of numerous philosophers.

From here, I will also have the opportunity to look at how current world events and mankind's foray into the digital and internet era have also been instrumental in the evolution of the privacy debate. I am keen to emphasize how modern day technology has served to add dimensions to the privacy debate that have never been previously encountered. An in-depth look at the technology itself will be necessary, utilizing material from a variety of sources.

A summary and analysis of the *Investigatory Powers Act 2016* will follow. A highly controversial piece of legislation, the initial parts of the Chapter

will be devoted towards highlighting the conflicting opinions and ideas that punctuated and influenced the drafting process. Through this, one will be able to frame the numerous political and moral stances on modern-day surveillance law and policy against the historical backdrop and arguments that I detailed in the Introduction chapter. I am keen to show how, despite the passage of time, the arguments remain – in their essence – the same. At this point, we also move to the central point of interest of the thesis and that is; whether the development that we have seen in surveillance technology been met with public, political and legal responses that account for the increased levels of *intrusiveness*? The thesis will seek to provide some insight into how nuanced these understandings and responses are.

By using the text of the Act and numerous supplementary documents (Explanatory Notes, Draft Codes, material from Government agency websites) there will be a summary of the numerous surveillance powers. There will also be a tentative discussion as to whether there is a tacit acknowledgment – whether through the words of the Act or the supplements – that some powers should be deemed as more *intrusive* than others. To finish this Chapter, there will be a general commentary on the Act, the bulk of which will be a discussion on how the permissions, judicial oversights and safeguards for each particular power differ, and whether this can provide further clarification on whether levels of *intrusiveness* were duly considered – producing a nuanced response in the legislation – from the drafters.

An in-depth look at Article 8 ('Right to Privacy') of the *European Convention on Human Rights* will follow. To start with, I wish to lay down how ECtHR jurisprudence has successfully included internet surveillance powers within the remit of Article 8 through the concomitant concepts of the 'Right to Data Protection' etc. The second half of the Chapter will include a close look at cases where State surveillance laws and systems have been brought before the ECtHR under Article 8. Parallels will be drawn between the material facts of these cases, the response from the Court and the powers and limitations inherent to the *Investigatory Powers Acts 2016.* The goal is to shed some light on the question of whether the Act would be considered illegal under Article 8, in line with ECtHR jurisprudence. Moreover, I wish to continue this look at *intrusiveness* (do they consider it?) and gauge whether the Court's approach is sufficiently nuanced and well-equipped to properly assess whether a modern day internet surveillance laws do or do not breach Article 8.

1 Introduction

1.1 (a) Key concepts: Safety and security vs. freedom and democracy

Big Brother is watching you.

George Orwell, 'Nineteen Eighty-Four' (1949)

The danger that mass surveillance poses to concepts of 'freedom' and 'democracy' have long been a topic of fiction as well as of hard academic study. George Orwell's Nineteen Eighty-Four is a work that some might disregard as mere post-apocalyptic whimsy but its arguably accurate recreation and prediction of the methods utilized by the totalitarian government to maintain absolute control over a population serves to give the novella a grim level of scholastic technicality and precision. The technology that forms the fictitious Ingsoc (English Socialism) government's central instrument of oppression was impossible at the time the book was composed. Known as the telescreen, it has the simultaneous function of a television, security camera and microphone. Government officials whose job it is to look for physical and mental signs of subversion permanently man it. It is present in the homes of all politically relevant members of society and cannot be turned off. Today, such technology is not only possible but all too real.[1]

The safety and security of the state and its population is the justification often touted by western democracies when confronted on issues of the development and implementation of increasingly sophisticated surveillance technologies. Such justifications have benefited from increased gravitas amid the concerns of international Islamic fanaticism, which, since the events on 9/11, have been an ever-intensifying phenomenon. To date, fifty-six deaths and three thousand and eighty-three deaths have occurred in the UK and the US respectively as a result of Islamist terrorist attacks since 1990. Whether these arguments for increased surveillance have any real substance is a matter of great contention.

[1]Indeed, parallels can be drawn between the telescreen and the Optic Nerve program developed by GCHQ in 2008, which indiscriminately 'intercepted and stored the webcam images of millions of Internet users.
(https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo)

In terms of justifications for surveillance measures, another parallel can be drawn with Nineteen Eighty-Four. It transpires that the Ingsoc government is subjecting its population to a state of wartime emergency. Citizens are constantly bombarded with telescreen propaganda, warning them of the dangers posed by foreign infiltration and underground revolutionary groups. There is some evidence to suggest that a war is indeed being waged with rival nations (at one point London is fire-bombed) but Orwell drops hints as to the fictional nature of the war throughout the novel, with attacks on the city merely being false-flags used by the government to justify and achieve popular support for their institution of increasingly oppressive measures. The uncertainty and sense of mystery inflicted on the reader as to the reality of the war or whether the material threat posed to the citizenry justifies this a state-of-emergency serves as an effective illustration as to the somewhat unfathomable and inscrutable nature of arguments justifying increased surveillance in the view of terrorist threats today. Is there a material connection between them? Are there any ulterior motives behind it?

Although I will concede that a strict comparison between Nineteen Eighty-four and modern Western society is somewhat overly dramatic, I feel the parallel serves to effectively highlight a key theme of this thesis and one that underlies its title; freedom and democracy vs. safety and security of the state. It is also poignant when one considers the fact that that, even in the 1940s, concerns on the use of surveillance technology as a tool of absolute oppression were present in people's (or Orwell's) minds given its limited development, compared to now. While Orwell's inspirations are generally cited as the means and methods of the Soviet regimes (and their secret police organizations such as the NKVD[2]) in maintaining control over a population, one wonders what types of surveillance practices and technologies were utilized at the time (and before) that could have influenced his envisioning of the telescreen and its nefarious usage, in England (the place of his birth).

Indeed, in order to provide the necessary information with which to give my thesis context, I believe a brief furor into the history of state surveillance methods and the reasoning for the implementation in England is necessary. Through this, I also hope to elucidate and compound some key concepts, which I will go on to explore in greater depth.

[2] Senyonovna, Eugenia (1967), *Journey into the Whirlwind*, New York: Harcourt, Brace & World, Inc.

1.1 (b) Key concepts: What are privacy and comparative intrusiveness?

What does privacy actually mean? The topic has been one of extensive philosophical discussion and unwary scholars can easily find themselves in a conceptual quagmire. To discuss the ins and outs of privacy is beyond the scope of the thesis. However, I do wish to draw attention to some ways in which ideas of privacy may manifest itself and how, some situations, may be considered more intrusive of privacy than others. This serves as preparation for a later Chapter in which, I shall be assessing how sensitive ECHR jurisprudence is in assessing forms of surveillance technology in view of these.

Privacy has been academically discussed in the context of property[3] and intimacy[4], with both of these elements possibly constituting elements of what some may call the private sphere or the private space. Indeed, the concept of privacy could be seen as the main influencing factor in the development of the common law maxim '…an Englishman's home is his castle' developed in Semayne's Case[5]. The case was germane to the development of the Tort of trespass. It was also succeeded by another landmark case, Entick v. Carrington[6], which – by virtue of this dictum – established limits to executive power and reaffirmed the rule of law, spearheaded by Lord Camden's famous statement: "If it is law, it will be found in our books. If it not to be found there, it is not law." The case in question details how 'the King's messengers' broke into the plaintiff's private property, caused extensive damage and confiscated property.

Heidegger's Critical Theory somewhat flies in the face of this through his contention that the private sphere is merely the place in which 'one can be one's authentic self' as opposed to the others that inhabit the public sphere.[7] In other words, it is the place in which one feels sufficiently comfortable to act and do with impunity. In this sense, the idea of privacy does not have a physical element per se, it is mental. An example of how the private sphere and the public sphere might converge is when one is taking a private phone call using a public telephone. The fact the operator of

[3] Janice Richardson (2017), *Law and the Philosophy of Privacy*, Routledge
[4] ibid.
[5] Peter Semayne v. Richard Gresham (1604), 77 ER 194
[6] John Entick, (Clerk) v. Nathan Carrington and Three Others (1765), EWHC KB J98
[7] Zizi A. Papcharissi (2016), *A Private Sphere: Democracy in a Digital Age*, John Wiley & Sons, Ch. 6

the phone is talking candidly about intimate subjects with friends and family would place the call within the private sphere despite the fact the location of the phone is physically located in – what many would refer to as – a public place.

This brief discourse on the nature of privacy provides the theoretic underpinning for the theory I wish to explore – that of comparative intrusiveness i.e. what makes an act a more serious violation of one's private life than another? I feel it is helpful to view violations of private life as not simply an end but also a means. For example, someone whose house is broken into will feel as if it is a violation of their privacy, even if that person had chosen not to take anything from it. Thus, the perceived violation can be described as means. Conversely, if someone picked up a personal letter from the ground in a public place, then engaged in a mass dissemination of its private contents, then it is not the means that is the key violation, in this case, it is the end. It is through this scope that we can attempt to qualitatively assess the privacy implications of different types of surveillance. This section does not seek to draw any conclusions on whether certain means or ends are more intrusive than others. It simply provides the framework from which one can assess legal response to breaches of privacy. As stated, the ultimate goal is to draw a conclusion on how sensitive the ECtHR is on such issues.

Below, I have attempted to create some categories that serve to highlight further how types of surveillance can be differentiated in terms of the means they employ and the content they harvest.

Targeted and non-targeted

The invention of CCTV in the mid-20th century arguably marked the first time when surveillance technology could be described as non-targeted; it enabling the indiscriminate observation of the public. Prior to this, the limitations of surveillance technology (such as the use of microphones for bugging or photographic equipment) meant that it was necessary to select a specific target - such as an individual suspected of committing a crime - beforehand. The same can be said for tracking devices, it requiring its physical placement on the person in question or their vehicle.

Clarke's description of personal data surveillance and mass data surveillance conveys a similar idea in the sense that; personal data surveillance "…monitors the

actions of one or more persons"[8] while mass data surveillance is "where a group or large population is monitored in order to detect individuals of interest."[9]

Active observation and passive recording

Some may seek to differentiate types of surveillance technology based on active observation (without recording the data in question) and passive recording (where observation of the recorded data may or may not occur at a later date). Where active observation is concerned, legal barriers will involve the use of the technology itself (planting a tracking device in a car, for example, may require that certain evidential standards are met beforehand). Conversely, where passive recording is concerned, legal checks will be in regard to access to previously recorded data, such as CCTV footage.

Private or public space

Whether surveillance technology is used in a private or public space may also be a matter of relevance. CCTV, for example, is commonly utilized in a public space, (a street) whereas the use of bugging devices on a landline phone would be an example of technology being used in a private space (such as in one's own home).

Public or private content

Finally, some may be tempted to specify types of data as public content and other types as private content. While some may see the difference as hinging on whether that data is retrieved from a public or private space, others may see it as being related to the topical content of the data in question and whether it can be perceived as being related to personal matters. Of course, in line with Heidegger's theorem, perhaps it is not the content itself that determines whether it is private, it is the fact that it was delivered on the presumption that it was private, and thus a person was operating within his personal sphere.

1.2 A brief history of state surveillance

The emergence of the first nation-states in the 16th century Europe saw an extensive use of undercover techniques to 'protect their political, military and

[8] Fuchs, C. & Boersma, K. (2012), *Internet and Surveillance, The Challenges of Web 2.0 and Social Media*, Routledge Studies in Science, Technology and Society, pp.1
[9] ibid.

economic interests.'[10] 'Special bureaus' were created by the state in order to collect intelligence on non-domestic enemies and rivals, a remit that bears a close resemblance to that of modern-day foreign intelligence agencies (such as UK's MI6). Such institutions engaged in practices such as opening diplomatic correspondence, recruiting informants as well sending spies 'to learn the secret intentions of their enemies and rivals.'[11] Although these surveillance techniques have seen use in all parts of the world for millennia[12], the fact that offices were being specifically designed by the state to organize its usage on a mass scale is foundational to modern day conceptions.

It wasn't until the creation of the first 'modern police apparatus[13]' in 17th century France that we see states directing mass surveillance practices towards their own populations in view of protecting public order. Police were instructed to collect information on 'potentially dangerous' people and groups via 'covert means'[14]. The institution of undercover policing polarized public and academic opinion. While early critics such as P. Manuel condemned it as tyrannical[15], high-ranking members of the police saw it as an invaluable tool to the proper carrying-out of their duties[16].

The state of undercover policing and state surveillance in England was far less developed at this time due to the maintenance of a 'traditional system of decentralized parish policing'.[17] When reform was proposed in the form of the Metropolitan Police Improvement Act in 1829 (so that England's system would be on par with France's 'modern system') it was met with much resistance by those who feared they would be subject to similar levels of state tyranny[18]. Conversely, numerous philosophers and jurists who had a hand in developing the Bill regarded it as a necessary evil to maintain order in the industrial age.[19]

The Bill was eventually passed by Parliament. Numerous initiatives were proposed, however, so as to render the English police as functionally distinct from

---

[10] Cyrille Fijnaut & Gary T. Marx (1995), *Police Surveillance in Comparative Perspective*, Kluwer Law International, pp.2, §5
[11] ibid.
[12] Soustelle, Jacques (2002), *The Daily Life of the Aztecas*, Phoenix Press, pp.209
[13] ibid.
[14] Cyrille Fijnaut (1979), *Opdat de macht een toevlucht zij? Een historische studie van het politie-apparaat al seen politieke instelling*, Kluwer Law International, pp. 489 – 551, 580 - 593
[15] P. Manuel (1790), *La police de Paris dévoilée*, J.B. Garnery
[16] Op.cit. Fijnaut & Marx
[17] J.J. Tobias (1979), *Crime and Police in England* (1700 – 1900), Gill and MacMillan, pp.25 – 56
[18] Op.cit. Fijnaut & Marx, pp.7
[19] L. Radzinowicz (1948 – 1956), *A History of English Criminal Law and its Administration from 1750*, London, pp. 417 - 522

France's. This was in an effort to alleviate the aforementioned worries and suspicions of the public[20]. One of these was to encourage an institutional focus on preventative policing as opposed to repressive policing[21]. Interpretations of this meant that the police forces were required to wear distinctive uniforms, resulting in a highly visible police presence as opposed to a secret police presence.[22]

Despite this, undercover policing was soon found to be a useful tool in conducting criminal investigations and the use of intelligence constables and detectives became increasingly common, as were the use of disguises (although not without strict orders[23]). This eventually led to the creation of a new department in 1878[24]. The remainder of the century saw the use of undercover policing become a matter of mere routine. This was encouraged by the perceived threat that Irish Nationalism and other popular movements had on the social order[25].

Covert policing was thrust into the limelight as the full details of the Soviet and Nazi legacy became apparent. As a result, it fell out of popular favor in Europe,[26] these regimes exemplifying the way in which the generalization and systematization of such tactics could be abused in order to subjugate a population. While they were being zealously developed and utilized in the US, modern European police forces were generally reluctant to follow their lead in response to this lack of popular support[27]. It was after President Nixon's declaration of a war against drugs that saw the police of Western Europe readopted covert police tactics with a renewed fervor.

The history of undercover policing and police surveillance in Europe reveals how the state security vs. freedom and democracy dichotomy has always been central to any debate on whether to increase or limit its usage. As mentioned, the Soviet Union (Orwell's key reference point for Nineteen Eighty-four) shows the severe repercussions of tipping the balance too much in favor of state security, which, as a by-product, criminalizes that which threatens the political status quo.

[20] Op.cit. Fijnaut & Marx, pp. 8
[21] S.H. Palmer (1988), *Police and Protest in England and Ireland 1780 – 1850*, CUP, pp.69 - 79
[22] Op.cit. Fijnaut & Marx, pp.8
[23] D.G. Browne (1956), *The Rise of Scotland Yard; A History of the Metropolitan Police*, George G. Harap, pp. 113 – 127, 182 – 196
[24] Op.cit. Fijnaut & Marx, pp.9
[25] ibid.
[26] ibid. pp. 15
[27] ibid.

1.3 From old surveillance to new surveillance; comparative intrusiveness

Coined by Gary T. Marx, new surveillance is defined as "the use of technical means to extract or create personal data. This may be taken from individuals or contexts." [28] By contrast, old surveillance refers to non-technical methods of surveillance such as those mentioned in Chapter 1.1 (the interception of letters, eavesdropping etc.).

Over the course of the 20th and 21st century, states have become increasingly reliant upon new surveillance methods to the point where old surveillance methods have largely fallen by the wayside. The methods themselves closely follow developing technologies, providing new ways through which personal data can be obtained, analyzed and accumulated.

The current generation of new surveillance provides access to a broader range of personal data, which is capable of being accumulated *en mass* whilst being analyzed and stored in its entirety. Moreover, the data can be replicated an unlimited number of times and sent to an unlimited number of people. I will explore the nature of the current generation of new surveillance in more detail in Chapter 1.3.

Other ways in which new surveillance can be distinguished from old surveillance is the way that is "less coercive" [29] in the sense that it can be carried out remotely thereby requiring no physical element (unlike eavesdropping or letter interception.). Thus, new surveillance can be considered easier and more readily available. Due to the affordable and accessible nature of sophisticated digital technology, new surveillance has also been characterized as "more democratized"[30], non-state actors and private individuals also being able to obtain and utilize surveillance methods. Finally, new surveillance differs from old surveillance in the sense that, with the latter, "the surveillant knows things the subject doesn't", [31] while the former tends to involve the subject knowing what the surveillant knows. [32]

Something, which I am keen to highlight, is the concept of comparative intrusiveness and what types of restrictions should be placed on the usage of

[28] Marx, Gary T., 'What's new about the "new surveillance"? Classifying for change and continuity' (2002), Surveillance and Society, Volume 1 (1): 9 – 29, pp.12)
[29] ibid, pp. 28
[30] ibid.
[31] ibid. pp.29
[32] ibid. pp.29

surveillance certain technologies in response to an arguably increasing degree of intrusiveness. As new surveillance develops and improves in the carrying out of its intended function, is the law adequately adjusting in response to this in order to protect people's rights, privacy, and autonomy?

I will continue by describing some forms of new surveillance technology and then describing how they can be implicated in a discussion of comparative intrusiveness and privacy.

1.4 Methods of new surveillance

1.4 (a) the pre-digital age

The development of the first photographic cameras (able to capture still and moving images), the first portable microphones, the first radio/telecommunications technologies and the first satellite technologies in the early-mid 20th century revolutionized the ways in which the police were able to collect and process evidence of criminal activity.

There are numerous instances of police agencies utilizing bugging or wiretapping in the course of criminal investigations; listening in to private conversations [33] through the interception of 'telecommunications, or electronic communications, or by using listening devices to overhear and record conversations.' [34]

States have also been known to access telecommunications data in the course of investigations. Telecommunications Service Providers (TSPs) store information relating to calls made by its clients such as their duration and frequency. Under certain circumstances, TSPs can be compelled to make this information available to the police. Such data can also be obtained through the use of metering devices. Police access to telecommunications data formed the crux of the ECHR case Malone v. the United Kingdom.

British police officials saw the potential use of photography as a tool for evidence gathering as early as 1895[35], with Sir Howard Vincent stating that 'the

[33] Peter Wright (1987), *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*, Stoddart, pp. 79 – 83
[34] ibid.
[35] Paul Knepper (2009), *Urban Crime Prevention, Surveillance, and restorative Justice: Effects of Social Technologies*, CRC Press, pp.82

utility of photography in the pursuit of criminals cannot be overestimated.'[36] Indeed, there are countless examples of still and moving photography forming an intrinsic part of criminal investigations throughout the 20th century. Photos stored in Britain's National Archives showed how London's Metropolitan Police subjected the suffragettes to a campaign of photographic surveillance who were regarded as, at the time, to be the 'biggest threat to the British Empire.'[37]

The emergence of the first satellite technologies in 1957 (when the Soviet Union launched the first ever artificial satellite into Earth's orbit) ushered in the development of the Global Positioning System (GPS). Any device containing a 'GPS receiving module' can have its precise coordinates remotely calculated. The surreptitious placement of these devices on vehicles or individuals can allow their exact locations to be recorded and stored. This data can then be analyzed the device's operator.[38] GPS tracking has seen extensive use by police to track and gather evidence on suspects.[39] It is also used as a form of punishment with courts ordering the attachment of electronic tags to convicted persons, enabling police to keep a constant eye on their movements.[40] The use of GPS tracking in a police investigation formed the basis of a case brought under the European Court of Human Rights (ECHR): Uzun v. Germany.

A technological descendent of moving photography, the very first Close Circuit Television (CCTV) systems emerged in the mid-20th century.[41] The earliest systems were unable to record footage and therefore required constant monitoring by human operators. This remained the case until 'magnetic reel-to-reel tape media'[42] was developed, which was subsequently replaced by the Analogue Video Cassette Recorder (VCR). CCTV cameras linked to a VCR could be left to passively record, leaving human operators free to review the footage at a later date.

---

[36] C.E. Howard Vincent (1900), *The Police Code and the General Manual of the Criminal Law for the British Empire*, Kent & Co
[37] Dominic Casciani, 'Spy Pictures of Suffragettes Revealed', BBC News Online, 3 October 2003 (http://news.bbc.co.uk/1/hi/magazine/3153024.stm)
[38] Gray (2013), *Leon, How does GPS Work*, The Rosen Publishing Group, pp.38
[39] Karen M. Hess (2013), *Police Operations: Theory and Practice*, Cengage Learning, pp. 106
[40] David Wright (2014), *Surveillance in Europe*, Routledge, pp.388
[41] Dornberger, Walter (1954), *V-2*, Ballantine, pp.14
[42] Kruegle, Herman (2011), *CCTV Surveillance: video Practices and Technology*, Butterworth-Heinemann, pp. 279

According to media reports, the UK is currently the 'most watched nation' by CCTV[43], with an estimated 1.85 million cameras in 2011.[44] The majority of these are owned and operated by 'private companies or individuals' with government cameras being numbered at a comparatively miniscule 52,000.[45] Whether these figures are accurate, however, is difficult to gauge given the fact the estimates vary greatly from source to source. It can be said with a matter of relative certainty that the government's ownership and operation of CCTV is comparatively limited to that of private actors.

1.4 (b) The Digital Revolution

The computerization of information that marked the digital revolution (the change from analog electronic technology to digital electronics) is said to have started somewhere between the 1950s and 1970s.[46] It completely revolutionized the way in which information was stored and transmitted. Photographic, video and audio surveillance were all now capable of being stored and transmitted in a digital format, presenting some key advantages over their analog predecessors.

One benefit of the digital format is that it enabled one to make infinite copies of the original data without suffering degradation in quality. This would be the same if one were to make a copy of a copy. Analog data, on the other hand, suffers from a phenomenon known as generational loss[47], each copy of a copy experiencing an incremental increase in degradation. Moreover, the process of making a digital copy is significantly easier than making an analog copy.[48] Another benefit of the digital format is that the original copy is less likely to experience any form of data corruption if stored properly. In the case of magnetic media (i.e. cassette tapes), the magnetic tapes will, over time, lose their magnetic orientation. This leads to the increasing degradation of the data in question.

The effectiveness of noise reduction techniques is the third benefit of digital media. Like analog data, digital data can suffer from noise, which is especially

---

[43] BBC News, 'UK, Most Watched Nation by CCTV', Tuesday, 21 July 2009, (http://news.bbc.co.uk/2/hi/uk/8160757.stm)
[44] See. Op.cit Colvin, Madeleine, *Under Surveillance*
[45] Big Brother Watch, 'The Price of Privacy: How local authorities spent £515m on CCTV in four years', 2002, (https://www.bigbrotherwatch.org.uk/files/priceofprivacy/Price_of_privacy_2012.pdf)
[46] Inder Sidhu (2016), *The Digital Revolution: How Connected Digital Innovations Are Transforming You Industry, Company and Career*, FT Press
[47] Richard W. Kroon (2014), *A/V A to Z: An Encyclopaedic Dictionary of Media, Entertainment and Other Audio-visual Terms*, McFarland, pp.310
[48] Peter Aksoy & Laura DeNardis (2007), *Informational technology in Theory*, Cengage Learning, pp.32

'prevalent in all analog and digital systems used for information communication, storage, and processing.'[49] However, with digital systems, this noise can be more 'effectively filtered.'[50] Whereas an analog audio recording may be rendered of no use due to noise, with no means of reducing it, in the case of a digital audio recording, methods of noise reduction may serve to render it useable.

Some other advantages include 1) high speed 2) high level of security and 3) simplicity of transmission[51] (see. the next chapter). In terms of surveillance, the invention of digital technology and usage in methods of surveillance (i.e. audio recordings and CCTV) can be seen as having numerous implications concerning privacy. For the first time, there existed the capacity for one's personal data to be reproduced in its original form ad infinitum, stored in posterity and, moreover, modified and transmitted much more reliably. It is at this point that we come to the computer age and the invention of internal and external network systems, otherwise known as the intranet and the Internet.

1.4 (c) The Computer Age

The Computer Age occurred parallel to The Digital Age and the terms are often used interchangeably[52]. For me, whereas the former epoch was more concerned with the development of the relevant technology, the latter is more a description of the time when information was subject to widespread computerization.

Over the course of The Computer Age, the capacity of digital technology to store[53], transmit[54] and compute[55] information experienced veritable leaps and bounds. Moreover, the epoch also encompasses the creation and proliferation of the first 'home computer' in the 1970s (the first one to appear in the USA entitled the Altair 8800). It saw immediate and overwhelming commercial success. Over the course of the century, 'home computers' have managed to infiltrate the vast majority of businesses, homes, government buildings, and research facilities. Today, over 83% of US households own a computer.[56] The fact that the computer became a

[49] ibid. pp.33
[50] ibid.
[51] ibid. pp.32
[52] See. Castells, M. (1999), *The Information Age, Volumes 1-2: economy, Society and Culture*, Oxford: Wiley-Blackwell
[53] Hilbert, Martin & López, Priscila, 'The World's Technological Capacity to Store, Communicate, and Compute Information', Science (2011). 332 (6025): 60–65.
[54] ibid.
[55] ibid.
[56] Lee Raine, 'Census: Computer ownership, internet connection varies widely across U.S, Pew Research Center' (2014) (http://www.pewresearch.org/fact-tank/2014/09/19/census-computer-ownership-internet-connection-varies-widely-across-u-s/)

veritable deus ex machina for all aspects of human life (home, work, and government) coupled with their popularity in the developed world eventuated in the radical expansion of the types and amount of personal data that was being digitally stored.

The invention of the Internet, and later, the World Wide Web in 1989[57] enabled it so that data could '…be collected, stored, analyzed, transferred, accessed, monitored, and solicited'[58] in large volumes and at terrific speed. It was not long before new types of surveillance technology were being developed in lieu of this era-defining invention. The surveillance capabilities one could possess by virtue of the mass usage of the World Wide Web were too great to ignore and it is not a hard task to foresee what ramifications such surveillance technology may have on issues of personal data protection/privacy. I will seek to explore this in more detail in the next chapter.

1.4 (d) the Internet and Surveillance

Table 1.1[59] in the book Internet 2.0 relates how the various 'qualities of the internet' serve to augment the surveillance capabilities of anyone seeking to use it for such a purpose. These 'qualities' are listed as including:

1) **Global communication:** one can remotely collect many 'data items' from 'certain individuals'[60] all over the world.

2) **Real-time global communication**: one can monitor communications as they happen, thereby allowing for the active 'coordination of social movements.'

3) **High-speed data transmission:** The existence of high-speed data transmission, allows for high-speed surveillance systems with large amounts of data being transferred globally.

[57] Bill Stewart, 'IPTO – Information Processing Techniques Office, The Living Internet', 2000, (http://www.livinginternet.com/i/ii_ipto.htm)
[58] Fuchs, Christian (2012), *Internet and Surveillance; The Challenges of Web 2.0 and Social Media*, Routledge
[59] ibid. pp.16 – 19
[60] ibid.

4) **Miniaturization:** due to the ever-increasing storage capacity and cheapness of chips, the amount of personal data that can be stored for personal surveillance is always increasing.

5) **Data multiplicity:** Something that was mentioned before, this term refers to the fact that personal data, via the Internet, can be copied 'easily, cheaply, and endlessly' and that 'copying does not destroy the original data.'[61]

6) **Multimedia:** This describes how the Internet is 'multisensory' nature, allowing such data as 'text, sound, image, animation, and video…' to be subject to surveillance through it.

7) **Hypertext**: Links between people can be 'more easily observed' as a result of the networked 'information structures.'[62]

8) **Online cooperation:** People share information and cooperate in projects which is something that could be subjected to surveillance.

9) **Decontextualisation:** Personal information may not be accompanied by suitable context, encouraging the practice of 'speculative and pre-emptive surveillance.'[63]

10) **Derealisation:** The line between fiction and reality can be blurred for surveillant. As a result, wrong interpretation may be made by the surveillant, which may subject the surveilled to increased scrutiny.

11) **Emotive Internet:** People express themselves through the Internet in an emotive fashion, rendering their intimate characteristics and emotions knowable to the surveillant.

12) **Ubiquitous Internet:** The Internet formed part of all aspects of daily life.

I have used streamlined definitions for some of these terms due to their largely self-explanatory, but for more information see. Pp.16 – 19, Fuchs,

[61] ibid.
[62] ibid.
[63] ibid.

Internet Surveillance 2.0). One thing that the table does effectively highlight is the pure power of the Internet and its complete suitability as a medium for surveillance activities. Through it, there are essentially no technological limitations as to the amount and type of personal data a person can duplicate, store, transfer, and monitor!

According to Starke-Meyerring and Gurak, there are 'three kinds of Internet surveillance technologies: 1) surveillance of personal data captured from general Internet use, 2) surveillance of personal data captured by using specialized Internet services…' and '3) technologies and practices designed to access data from Internet users.'[64] I will go on to look at these in some detail.

1.4 (e) Internet surveillance tools

Although the global intelligence community remain reticent in concern to the means and methods of Internet surveillance they choose to employ in the course of their duties (as well as any new methods being developed with their oversight), the ways in which government agencies are able to remotely monitor Internet communications is by no means a mystery to a significant minority of the general population. This is not only by virtue of the various leaks of classified government information that has occurred over the years (such as the Ed Snowden debacle[65]), but also because such methods have been employed by so-called civilian hackers (for testing network security measures) ever since the world wide web became a matter of public access.[66] Notwithstanding, the methods employed by crackers and hackers to remotely access information and communications derive from similar practices employed on internal and local networks that existed beforehand. Indeed, people were employed to implement network security measures and test them (something known as security hacking) since its invention.

Spyware is a variety of malware (malicious software), which is specifically designed to gather personal data without the subject's knowledge and may also reproduce and sent it to other entities without the subject's consent.[67] One

---

[64] Starke-Meyerring, Doreen and Laura Gurak (2007), *Internet Encyclopedia of privacy*, Greenwood Publishing Group, pp.297-310

[65] James Ball, 'Leak memos reveal GCHQ efforts to keep mass surveillance secret', The Guardian, 25 Oct 2013, (https://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden)

[66] See. Kevin D. Mitnick (2011), *The Art of Deception: Controlling the Human Element of Security*, John Wiley & Sons

[67] See. 'Monitoring Software on Your PC: Spyware, Adware, and Other Software, Staff Report: Federal Trade Commission' (2005) (https://www.ftc.gov/sites/default/files/documents/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-and-other-software-report/050307spywarerpt.pdf)

variety of spyware is known as the Trojan horse given the fact that the software is specifically designed to mislead the subject as to its true nature, thus allowing the user surreptitious access to personal data. The Trojan horse may be disguised as a benign download[68] or email attachment (emails sent repeatedly and deliberately with the intent of infecting subjects' computers with malware is often termed spam). They can collect many types of data, including but not limited to: Internet surfing habits, user logins, and credit card information.

Phishing describes the practice of tricking subjects into providing sensitive information. This method is particularly interesting in the sense that shows how methods of Internet surveillance don't necessarily have to be technological, instead relying on traditional subversive methods which would have been used in the times preceding new surveillance (see. chapter 1.4). The key differences between phishing and old surveillance methods lie in the fact of the Internet's speed, derealisation, decontextualization, ubiquity and it's multimedia capabilities (see. chapter 1.4(d)); meaning that phishing can certainly be argued to be more intrusive than an undercover policeman or spy.

Phishing often takes the form of an email or an instant message, which is disguised so as to appear to be from a trustworthy source (such as a bank or government agency). The email will often ask the subject to provide their passwords and credit card details. The subject, being convinced by the message's apparently legitimate nature, will willingly oblige. The sender will then use the information for malicious purposes. [69]

Packet sniffers are types of hardware or software that can be used to 'grab' packets of data from any kind of network, including the Internet. Typically they are used for network related diagnostics such as monitoring traffic or being notified for potential intrusions. In terms of surveillance capabilities, they can be used for the collection of sensitive information such as login details and 'what information is being exchanged between two parties.' [70]

No reference is given to any of these three surveillance methods in related UK legislation. Indeed, as I will go on to elucidate later in the thesis, such legislation as the Investigatory Powers Act 2016, provides absolutely no detail as to the specific means and methods employed by security agencies in the course of Internet surveillance. Instead, these are encapsulated by the extremely broad terms: 1)

[68] ibid.
[69] ibid.
[70] Andy O'Donnell, 'What are Packet Sniffers and How Do They Work?', 2018, Lifewire, (https://www.lifewire.com/what-is-a-packet-sniffer-2487312

interference and 2) interception. That said, these terms do serve to include such methods as malware, phishing and packet sniffers within its ambit, in line with their very implied meaning (interference, for example, is often mentioned in the context of physical equipment which does bear a close resemblance to the practice of packet sniffing). Of course, this is mere speculation and this is one of the frustrating things about the UK's surveillance legislation. Of course, depending on the specific methods employed, it may alter the perception of whether the act itself is more or less intrusive and, thus, more or less deserving of restriction. If the methods are hidden in vague terms, then this is much harder to do.

Another method of Internet surveillance is known as ISP (Internet Service Provider) log file access. ISPs are commonly understood as "'an organization that sells access to the Internet.' – an access provider."[71] Some examples of ISPs include BT in the UK or Telia in Sweden. Such organizations are able to maintain logs (in the forms of a Uniform Resource Locator (URL) or every webpage their clients visit, the length of the time they spend on them and the searches they make. This is made possible through monitoring the requests made by the client's Internet protocol (IP) address to other IP addresses (such as a website). An IP address is assigned to the client upon subscription to the service and represents the location of the client's device (such as a computer or mobile phone) on the network. Naturally, the ISP knows or can find out the name client's name and location. These logs can be stored for an indefinite period and can be requested by/sold to third parties.

IPS log file access is directly referred to by UK surveillance legislation within provisions concerning 'data retention' and 'obtaining communications data'. They stipulate measures on the IPS mandatory retention of ISP log files, as well as the circumstances in which they can be provided to security (and other government agencies). I will go into more detail on the precise meaning of these terms in the next chapter.

The next method of Internet surveillance I wish to highlight is known as Open Source data collection. This refers to data that is freely accessible on the Internet or otherwise and the collection of this data through human or automated means. The data in question then can be stored, replicated, analyzed and transmitted. One might be tempted to liken this method of Internet surveillance with CCTV cameras, passively observing and recording public activity. The aforementioned qualities of the Internet make open source data collection arguably much more

[71] ibid.

intrusive and insidious, however. These qualities include the derealized, the decontextualized, and emotive nature of the Internet, coupled with the multimedia aspect and its data multiplicity capabilities (see. Chapter 1.3(4)).

Given the fact the personal information in question is being willingly and knowingly placed in a public space (although whether the Internet can be considered a public or private space is still a matter of debate, especially concerning social networking sites[72]) whereby it can, without the usage of hacking, be subject to surveillance (not only by the government but also members of the public), invite the question of whether legal safeguards should actually exist for this method of surveillance. In terms of UK surveillance legislation, there is a distinctive hole in this regard. In terms of CCTV, there are safeguards in concerning the installation of the cameras as well as access to the recorded data. Given the nature of the Internet and their surveillance ramifications, should not such legal limitations also exist for the surveillance of open source data? One might claim that this should not be the case, given the fact that the data available is subject to knowledge and consent, unlike with CCTV footage.

Whether legislation safeguarding against the surveillance of open-source data should be enacted is beyond the scope of this Chapter, but it does serve to highlight the relevance of debates concerning what constitutes privacy as well as whether one form of surveillance can be considered more or less intrusive than another, and what methodology should be applied in order to determine this. I do not wish to abandon this very important debate, however, and I will go one to consider it as part of a separate chapter.

1.4 (f) Conclusion to the overview

I feel that the preceding chapter goes to provide a useful theoretical starting-point from which to cast a critical eye at the main topic of the thesis; the legality of the Investigatory Powers Act 2016 under Article 8 European Convention of Human Rights (ECHR). After a discussion of its legality, I will seek to engage in the date of whether the European Court of Human Rights' (ECtHR) jurisprudence is adequately equipped to fully and adequately engage with concepts of privacy in relation to the various methods that go to constitute the phenomenon known as internet surveillance. Primary to this debate are considerations of the ECtHR's

[72] Jean Camp, 'The Internet as a Public Space: Concepts, Issues, and Implications in Public Policy', John F. Kennedy School of Government, Harvard University, 2000, (https://sites.hks.harvard.edu/mrcbg/research/j.camp_acm.computer_internet.as.public.space.pdf)

interpretation of privacy in line with the ever-evolving alternatives, as well as, to what degree, they fully engage and apply the concept of the comparative intrusiveness when considering methods of surveillance. Have they fully accounted for the wide-ranging implications of the Internet?

2 The Investigatory Powers Act 2016

2.1 Overview

The Investigatory Powers Act 2016[73] (IPA 2016) is the latest in a long line of legislation geared towards providing the government, the UK Intelligence Community, and police agencies with a veritable tool-kit of surveillance powers, including but not limited to internet surveillance. I will embark on a detailed overview of the Act, it superseding and amending all previous surveillance and investigatory legislation to form the legal keystone of the UK government's on-going surveillance regime. Once I have outlined its most important elements, I will analyze the Act in relation to its legality under Article 8 ECHR and provide further commentary on notions of comparative intrusiveness; is ECtHR jurisprudence sufficiently well equipped to deal with the privacy ramifications of internet surveillance legislation such as this?

2.1 (a) Preceding Legislation

The IPA 2016's legal ancestors reveal how susceptible surveillance powers are to increasing state security concerns (especially those related to terrorism and other forms of serious criminality) and developing technology. Over the course of time, surveillance powers have seen a gradual expansion, addition, and amendment in response to these factors, with the IPA 2016 being its latest incarnation. This stream of legislation started with The Regulation of Investigatory Powers Act 2000[74] (RIPA) and was followed by; The Terrorism Act 2006, The Serious Crime Act 2007, The Counter-Terrorism Act 2008, The Policing and Crime Act 2009, The Terrorism Prevention and Investigation Measures Act 2011, The Data Retention and Investigatory Powers Act 2014[75] (DRIP), The Counter-Terrorism and Security Act 2016 and The Serious Crime Act 2016.

The earliest of these acts, RIPA, was drafted precisely to help the police and security services adequately deal with the growth of Internet

[73] The Investigatory Powers Act 2016
[74] The Regulation of Investigatory Powers Act 2000
[75] The Data Retention and Investigatory Powers Act 2014

communications and the development of new methods of encryption at the beginning of the new millennium.[76]

RIPA covers a range of surveillance methods within five broad categories, including methods of old surveillance[77]. Two of these five categories were particularly controversial, they being the first of their kind to consolidate methods of Internet surveillance in substantive law. They are referred to by the Act as 'the acquisition of communications data (e.g. billing data) and 'the interception of communications'.[78]

In 2014, its equally controversial successor, DRIP, legislated an additional category known as enforced 'data retention'.[79] Instead of the DRIP being drafted in response to a burgeoning technological development, it was in fact rushed[80] through Parliament in order to retain numerous data retention powers in the aftermath of a European Court of Justice (ECJ) decision. The decision effectively struck down the EU's Data Retention Directive[81] whose main objective was to 'harmonize Member States' provisions concerning the retention of certain data…'[82] As such, advocates of DRIP insisted that it was doing no more than preserving 'the status quo' [83], with EU law having already laid the groundwork for the implementation of such powers. Moreover, many supporting Members of Parliament (MPs) lauded the Act's facilitation of numerous powers that were seen as necessary in tackling a heightened terrorist threat as well as pedophilia[84].

In a High Court ruling[85], The DRIP was subsequently found to be in contravention of EU law and ordered that the act should be 'disapplied'. The decision was based on the fact that s.1 of DRIP did not 'lay down clear and precise rules

---

[76] Unknown, 'Regulation of Investigatory Powers Act 2000', The Guardian, Monday 19 January 2009, (https://www.theguardian.com/commentisfree/libertycentral/2009/jan/14/regulation-investigatory-powers-act)

[77] The Act, for example, legislates for 'the use of covert human intelligence sources (agents, informants, undercover officers)', 'Regulation of Investigatory Powers Act 2000; Explanatory Notes', Chapter 23, §3, (http://www.legislation.gov.uk/ukpga/2000/23/notes)

[78] ibid.

[79] Data Retention and Investigatory Powers Act 2014, Section 1

[80] 'Commons passes emergency data laws despite criticism', BBC News, 15 July 2014 (http://www.bbc.co.uk/news/uk-28305309)

[81] Council Directive 2006/24/EC on the retention of data generated or processes in connection with the provision of publicly available electronic communications services or of public communications networks and amending [2006] L105/54

[82] Press Release No 54/14, 'The Court of Justice declares the Data Retention Directive to be invalid', Court of Justice of the European Union, 8 April 2014 (https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf)

[83] Op.cit. BBC News, 15 July 2014

[84] ibid.

[85] Davis & Ors v. SSHD [2016] EWHC 2092

providing for access to and use of communications data'[86] which was the same reason the aforementioned directive was struck down by the ECJ. It was this that prompted the developments of the IPA's draft bill.

The three categories of Internet surveillance previously highlighted, 1) acquisition of communications 2) interception of communications and 3) data retention, form an enduring element of the IPA. Decidedly vague in nature, covering a range of powers and obligations, I will seek to examine these in more detail in future sections.

2.1 (b) The Drafting of the Act: Parliamentary debate and public responses

The draft bill, dubbed by many media houses as the 'Snooper's Charter'[87], caused something of a furor with the seemingly 'wide-ranging spying powers'[88] it grants the UK's intelligence agencies, the police, and numerous other government bodies. Terms such as 'extreme surveillance'[89] have been frequently employed to describe its content, accompanied by claims that it is 'unmatched by any other country in Western Europe…or the US'[90] and that it is a 'beacon for despots everywhere.'[91] Many have highlighted the speedy and quiet fashion though which the draft bill was proposed, debated and passed through Parliament, it only gaining wider public attention until it was already law. Some have interpreted this as a deliberate tactical decision, the implication being that the government was worried about public scrutiny beleaguering its passage.[92]

---

[86] ibid. § 114

[87] Griffin A., 'U.K. spying laws: government introduced law requiring WhatsApp and iMessage to break their own security', The Independent, 12 March 2016 (http://www.independent.co.uk/life-style/gadgets-and-tech/news/uk-spying-laws-uk-government-introduces-law-requiring-whatsapp-and-imessage-to-be-broken-a6905106.html)

[88] Griffin, A., 'Investigatory Powers Act Goes Into Force, Putting UK Citizens Under Intense New Spying Regime', The Independent Newspaper, 31 Dec 2016 (http://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-act-bill-snoopers-charter-spying-law-powers-theresa-may-a7503616.html)

[89] MacAskill, Ewen, 'Extreme surveillance' becomes UK law with barely a whimper', The Guardian, 19 Nov 2016 (https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper)

[90] ibid.

[91] Op.cit. Investigatory Powers Act goes into Force, The Independent

[92] Griffin, A. 'The Government Quietly Launched 'Assault on Freedom' While Distracting People, Say Campaigners Behind Legal Challenge', The Independent, 9 Jan 2017 (http://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-act-liberty-legal-challenge-high-court-opposition-a7518136.html)

Members of Parliament (MPs) who opposed the passing of the IPA's draft bill have vocalized the concern that 'the surveillance activities proposed…go way too far and too fast…are vaguely described, disproportionate and lack critical safeguards.' [93] One way in which the IPA draft bill was considered as going too far was in the way that the act does not merely concern 'national security, crime, and public safety', it also involves itself in 'a long list of other purposes – from tax collection to economic well-being and public health' with ICRs being made available to a long list of government agencies, other than the police and security services including Her Majesty's Revenue and Customs (HRMC) and the National Health Service (NHS).[94]

Other MPs have echoed arguments previously made by infamous whistle-blower Edward Snowden, suggesting that such legislation casts the net too wide, it resulting in the harvest of an amount of data far too inordinately large to be of any use to the security services. As such, it is deemed 'counterintuitive' due to the fact that the likely result will be a worsening 'in their work rate.' [95] Criticism has also concerned the draft bill's weak provision of a 'judicial oversight of powers'[96].

The bill's proponents, on the other hand, hold it as vital to the work of law enforcement and the security services [97] whilst providing for 'stronger safeguards and greater openness'[98]. Indeed, many of the justifications made for the IPA are in the same vein of those made for RIPA; that such laws are necessary in order to cope with an increasingly sophisticated breed of criminal and terrorist in this '…digital age' [99] we now live in. The usage of digital technology by criminal enterprises and terrorist organization in order to increase the efficiency and secrecy of their activities is an undeniable fact. Prima facie, it makes complete sense that legislation should constantly be amended and expanded in order to stay ahead of the increasing sophistication of terrorists and criminals. One only needs to do some rudimentary research into the ISIS propaganda machine to see how the Internet can

[93] Baroness Jones of Moulsecombe, 'Data Retention and the Investigatory Powers Bill', House of Commons Debate, 15.07.2014, Column 319
[94] ibid.
[95] ibid.
[96] The Lord Bishop of St. Albans, 'Queen Speech Debate in the Lords Chamber', 24.05.2016, Column 284
[97] 'Investigatory Powers Bill: Context', (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/530551/Context_Factsheet.pdf)
[98] ibid.
[99] 'Investigatory Powers Bill; Factsheet; Targeted Communications data', (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473747/Factsheet-Communications_Data_General.pdf)

be effectively utilized to influence and orchestrate worldwide terrorist attacks and 'radicalize and recruit'[100] young, disaffected men and women.

MI5 chief, Andrew Parker, has testified as to the efficacy of such legislation in the fight against criminality and terrorism, insisting that certain provisions within the act will 'help join the dots in complex…investigations'[101] which, in turn, 'saves lives.'[102] Indeed, there has been a general governmental insistence that, without the IPA, crimes 'enabled by email and Internet will go undetected and unpunished.'[103]

This viewpoint has received wide acknowledgment by numerous politicians and other security officials. Indeed, it was reported that powers included in the IPA are 'used in 95% of serious and organized criminal investigations handled by the Crown Prosecution Services (the CPS)'[104] and has 'played a significant role in every Security Service counter-terrorism operation over the last decade.'[105] It has also been claimed to be effective in the arrest of 'repeat burglars, robbers and drug dealers.'[106] Reference is also made to a number of infamous murder, terrorist and child grooming cases where communications data (a component part of the IPA and RIPA) has played an important part including the: Oxford and Rochdale child grooming cases[107], the murder of Holly Wells and Jessica Chapman[108] and the 2007 Glasgow Airport Terror Attack.[109] Parliamentarian, Yvette Cooper, highlights that

---

[100] 'Investigatory Powers Bill; Factsheet; Targeted Interception', (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473739/Factsheet-Targeted_Interception.pdf)
[101] Op.cit. Factsheet; Targeted Communications data
[102] Weaver, M., 'MI5 resisting independent oversight of bulk data collection', The Guardian, 26 July 2016 (https://www.theguardian.com/uk-news/2016/jul/26/mi5-resisted-independent-oversight-of-communications-data-collection)
[103] ibid.
[104] May, Theresa, 'Data Retention and the Investigatory Powers Bill', House of Commons Debate, 15.07.2014, Column 736
[105] ibid.
[106] Home Office, 'Factsheet #1 – Communications Data; Data Retention and Investigatory Powers Bill', 2014,pp.1 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/330510/Factsheet_Data_Retention.pdf)
[107] Home Office, 'Retention of Communications Data Codes of Practice', 9 December 2014, pp.2, (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/383401?Draft_Data_Retention_Code_of_Practice_-_for_publication_2014_12_09.pdf)
[108]Sir Ronnie Flanagan, 'A Report on the Investigations by Cambridgeshire Constabulary into the Murders of Jessica Chapman and Holy Wells at Soham on 4 August 2002; Summary of Conclusions and Recommendations' (2002), §5.71, pp.16 (https://www.justiceinspectorates.gov.uk/hmicfrs/media/investigation-by-cambridgeshire-constabulary-20040530.pdf)
[109] House of Lords & House of Commons Joint Committee on the Draft Communications Data Bill, 'Draft Communications Data Bill' (2012 – 13), pp.8

recent Child Exploitation and Online Protection Centre investigations have resulted in the arrest of '200 suspects and identified 132 children who were at risk of abuse'[110] through the use of communications data. She compares this against the success rates of German police of whom, not possessing such rights of access, have only been able to investigate 'a handful of cases.'[111] Indeed, communications data is claimed to be utilized by the UK police in the course of 1) 'piecing together the activities of suspects, victims and vulnerable people' 2) 'proving or disproving alibis' 3) 'identifying links between potential criminals' 4) 'tying suspects to a crime scene' and 5) 'finding a vulnerable person who is at risk of imminent harm.' [112] Notwithstanding, the IPA has also been praised for increasing the transparency of such activities, making powers, which were previously a 'closely guarded', a matter of public knowledge.[113]

As is revealed by public and political responses the draft bill of the IPA the argument boils down to safety and security vs. freedom and democracy, as was highlighted in Chapter 1.2. It is beyond the ambit of this chapter to decide on whether the provisions included in the IPA have struck the correct balance in reference to these dual standards. The opinions I have related, however, will provide some fuel towards considerations of necessity, a concept that I will engage with upon my analysis of ECHR jurisprudence later in the thesis.

2.2 The IPA 2016; overview and structure

The IPA 2016 is an extensive piece of legislation, the text of the Act consisting of precisely 291 pages. These are divided into nine Parts, with each Part also being segmented into numerous Chapters, Sections, and Subsections (i.e. IPA 2016, Part 2, Chapter 1, Section 18, §1 (a)). The Parts functions as the main clauses of the Act. Following the main clauses are ten Schedules. These are used to go into greater detail on how the preceding clauses are to be implemented in practice. These are also divided into Chapters, Sections, and Subsections.

In this section of the thesis, I will attempt to succinctly highlight and summarize the salient elements of the Act in relation to its implementation of laws

[110] Cooper, Yvette, Data Retention and the Investigatory Powers Bill, House of Commons Debate, 15.07.2014, Column 719
[111] ibid.
[112] Op.cit. May, Theresa, Column 704
[113] David Anderson, 'A Question of Trust; Report of the Investigatory Powers Review', Independent Reviewer of Terrorism Legislation, 2016, (https://terrorismlegislationreviewer.independent.gov.uk.uk/wp-content/uploads/2015/06/IPR-report-Web_Accessible1.pdf)

relating to Internet Surveillance methods. Instead of approaching the Act clause by clause chronologically, thereby merely condensing reams of text, I will be going in-between Parts, utilizing the Act's Explanatory Notes and the aforementioned Schedules. This is not only for the sake of brevity; it is also to elicit the Act's true and accurate meaning. Notwithstanding, a lot of the following text will be an interpretation of how the Act can be divided so as to show each individual Surveillance tool it legislates for, how they can be used and their implications regarding the Right to Privacy. Moreover, in order to aid this interpretation, I will also be utilizing non-source 3rd party material so as to try to adequately define terminology that the Act arguably hazards to leave ambiguous in meaning.

Before commencing, it is important to note that the IPA 2016 is not intended to strictly apply the Internet. Indeed, the usage of such non-internet-specific terms such as 'telecommunications' and 'telecommunications operators' means that the inclusion of Internet communications within the Act's ambit is implied instead of express. This is obviously done to avoid the exclusion other technologies such as wireless telegraphy (radio) and the telephone. This is understandable given that, as mentioned earlier, the IPA 2016 is considered as an update to legislation enacted in the pre-internet era. For the purposes of this thesis, 'telecommunication operators' will be taken to mean 'Internet service providers' (ISPs) of whom 'provide services where customers, guests or members of the public'[114] are provided with access to Internet services.

2.3 (a) The alternate forms of Internet Surveillance in the IPA 2016

Parts 2 – 5 are the meat of the Act, serving to describe and divide it into, what I deem to be, five main categories of Internet surveillance powers. These five main categories of Internet surveillance are as follows:

- 'Interception of communications'[115]
- 'Obtaining communications data'[116]
- 'Retention of communications data'[117]

[114] Home Office, 'DRAFT Code of Practice; Interception of Communications', December 2017, §2.7, pp.7, (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/668941/Draft_code_-_Interception_of_Communications.pdf)
[115] IPA 2016, Part 2
[116] ibid. Part 3
[117] ibid. Part 4

- ‘Equipment Interference’[118]
- ‘Bulk personal datasets’
- ‘Targeted and bulk powers’

Prima facie, the headings of these Parts may seem fairly self-explanatory in what they permit or, conversely, disconcertingly broad. Indeed, those with knowledge of the technological tools that companies and institutions have at their disposal may err on the side of these being too broad. To the contrary for those that have no such knowledge; they might imagine the process of interception to be a fairly linear affair and have minimal desire to explore this further. In any case, I will go through these categories in turn and elicit their meaning in more detail by analyzing the precise terminology applied within the context of the Act. I will start by analyzing the meanings of ‘Interception’, ‘Obtaining’, ‘Retention’, ‘Interference’, ‘Bulk personal Dataset’ and ‘Targeted and bulk powers’.

2.3 (b) ‘Interception of communications’

Interception is defined as acts, which include ‘modifying or interfering with the system and monitoring transmission made by means of the system.’[119] Inherent to the definition is that the consequence of the acts in question ‘must be to make the content of the communication available to a person who is not the sender or the intended recipient.’[120] The act must be committed at the ‘relevant time’[121] which is dictated as meaning any time in which the ‘communication is being transmitted or any time when the communication is stored in or by the system.’[122] With reference to digital communications, the term ‘system’ refers not only to Internet servers but also the storage memory of digital devices such as phones or tablets of either the sender or the recipient.[123] Thus, ‘interception’ can occur at every point in the timeline of a communication’s drafting, transmission, and arrival, using any/all technological means to retrieve the communication in question.

If one takes an email as an example of a communication, the Act differentiates between the forms of ‘data’ that can be taken from it. These are ‘content data’ and ‘secondary data.’[124] ‘Content data’ is fairly self-explanatory, it

[118] ibid. Part 5
[119] ibid. Part 1, Section 4, §2
[120] ibid.
[121] ibid. §3
[122] ibid.
[123]Op.cit RIPA 2000; Explanatory Notes’, pp.14, §41
[124] ibid. Part. 2, Chapter 1, Section 15

simply consisting of the transmitted content whatever it may be (text, photo, voice recording etc.). Secondary data should be '…comprised in, included as part of, attached to or logically associated with the communication'[125] but should not reveal the 'meaning' of the communication itself[126] (i.e. the message contained in an email remains private) and is considered '**less intrusive** than content' data.[127] Secondary data is divided into types; 'systems data or identifying data.'[128]

'Identifying data' refers to any 'data, which may be used to identify, or assist in identifying any person, apparatus, system or service…any event…or the locations of any person, event or thing.'[129] With reference to 'event', identifying data can be used to establish the fact of its existence, 'the method or pattern of the event'[130] and 'the time or duration of the event.'[131] In real terms, one could use an example of a digital photograph. Data attached to the photograph may be used to identify the date it was taken (i.e. a digital time stamp) or where it was taken (i.e. network location data) which could lead to the identification of the person who took it. This can be achieved without actually seeing the photograph itself.

'Systems data' is 'data which enables or facilitates, identifies or describes anything connected with enabling of facilitating' [132] the function of a 'telecommunications system.' [133] This description does not mean much to the layman, whether he is a legal professional or otherwise. Indeed, without an in-depth knowledge of how network infrastructures work, it is difficult to ascertain to what extent the surveillance of such data can potentially infringe notions of privacy. The Act's DRAFT Code of Practice refers to the use of an application on a phone as an example, the 'systems data' being the data exchanged between the phone and the 'application server, which makes the application work in a certain way.'[134] 'What might this materially say about a person?' is a question that is tough to answer.

2.3 (c) 'Obtaining communications data'

[125] ibid. Section 16, §5
[126] ibid. §6(c)
[127] Op.cit. 'DRAFT Code of Practice; Interception of Communications', pp.7, §2.12
[128] Op.cit. RIPA 2000; Explanatory notes, §67
[129] Op.cit. IPA 2016, Part 9, Chapter 2, Section 263, §2 (a) – (c)
[130] ibid. §3 (a) – (c)
[131] ibid.
[132] ibid. Section 263, §(4)
[133] ibid. §(4)(a)
[134] Op.cit. 'DRAFT Code of Practice; Interception of Communications', pp.8, §2.13

Contained in Part 3 of the IPA 2016, this power enables the authorities to 'obtain…communications data from a telecommunications operator.' [135] Unlike 'interception', the power to 'obtain' implies the cooperation, facilitation, and knowledge of the telecommunications operator. Indeed, in simple terms, the authority makes a demand for the data in question and telecommunications operator provides it. I will explain the finer details later in the chapter.

'Communications data' is described as the 'who, where, when, how and with whom of communications, but not its content.'[136] Communications data is divided into two subcategories: 1) entity data and 2) events data. The former concerns identifiers associated with the customer accounts of telecommunication services. In terms of Internet services, this would include Internet Protocol Addresses (IPs), something that is allocated to customers by the service provider.[137] The latter refers to 'the fact that someone sent or received an email…text or social media message. It also includes data relating to which Wi-Fi hotspots the device connected to.'[138] Moreover, entity data also consists of 'internet connection records' which can be used to demonstrate whether a certain device connected to a certain website or 'accessed an online communications system.'[139] Despite this, such data cannot be used to determine what the individual did on that service.

In the DRAFT Code of Practice, communications data is implied as being an element of secondary data, with secondary data constituting a 'broader category of data.' [140] It is logical to suggest that secondary data encompasses both the aforementioned entity and event data.

2.3 (d) 'Retention of Communications data'

Part 4 Section 87 of the IPA 2016 '…provides a power to require telecommunications operators to retain communications data.'[141] Once the power has been invoked, selected communications data must be retained for a maximum of 12 months.[142] This can then be 'obtained' via the aforementioned legal means.

---

[135] Op.cit IPA 2016, Part 3, Section 67, §(1)(b)
[136] Op.cit. RIPA 2000; Explanatory Notes. §174
[137] Home Office, Factsheet: data definitions, Investigatory Powers Bill: fact sheets (2016), (https://www.gov.uk/government/publications/investigatory-powers-bill-fact-sheets)
[138] ibid.
[139] Op.cit. RIPA 2000; Explanatory Notes, pp.41, §265
[140] Op.cit. 'DRAFT Code; Interception of Communications', pp.7, §2.12
[141] Op.cit, RIPA 2000; Explanatory Notes, pp.41, §265
[142] Op.cit. IPA 2016, Part 6. Section 87, §3

2.3 (e) 'Equipment Interference'

Found in Part 5 of IPA 2016, 'equipment interference' is described as a 'range of techniques…that may be used to obtain communications, equipment data or other information from the equipment.'[143]

Equipment data is synonymous with Secondary data, as described in 2.4(a), covering both systems data and identifying data.[144] There is no indication as to what 'other information' might consist of. The implication is that there is no limit as to the types of information/data that can be extracted from 'equipment', this Part of the Act seems to include all of the previously mentioned data types within its ambit. This differs sharply from the provisions described in 2.3 (b) and (c) which requires the obtaining of 'communications' and 'communications data'/'secondary data' to be done through alternate legal avenues. It was my presumption that this was the case due to recognizing of the comparative 'intrusiveness' of these two different types of data. The fact that Part 5 does not seem to divide types of data in this way arguably goes to contradict this.

The definition of 'equipment' is extremely broad. Described by section 135 of the Act as anything producing 'electromagnetic, acoustic or other emissions'[145], this essentially goes to include any electronic device that one can feasibly imagine. 'Interference' is stated as including 'a range of techniques' that 'can be carried out either remotely or by physically interacting with the equipment.'[146] Again, this is very broad, but the DRAFT Code provides some helpful examples of equipment interference.[147] Both examples do not make specific reference to either the Internet or networked communications. Prima facie, it may seem as if this method of surveillance is not particularly relevant to the thesis topic. Notwithstanding, the examples do make reference to the concept of 'remotely installing'[148] surveillance software (also dubbed spyware) such as a 'keylogger'[149]. The remote installation of software on equipment is made possible through the Internet via the Trojan horse method mentioned in Chapter 1.4 (e) of this thesis. An email might be sent to the target including a file attachment designed with the intention of tricking them into

[143] Home Office, 'DRAFT Code of Practice; Equipment Interference', Autumn 2016, pp.8, §2.3, (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/668940?Draft_code_-_Equipment_Interference.pdf.)
[144] ibid. pp.9, §2.11
[145] Op.cit. IPA 2016, Part 5, Section 135, §1(b)
[146] Op.cit. 'DRAFT Code; Equipment Interference', pp.8, §2.4
[147] ibid.
[148] ibid.
[149] See ibid.

downloading it. The surveillance software is thereby surreptitiously installed onto the equipment in question.

The data obtained through 'equipment interference' is not necessarily related to one's activity on the Internet or networked communications (although it can in a sense). Instead, the Internet is used as a vehicle for obtaining any and all data connected with the existence and usage of an electronic device. While key-logging software can detect and record everything you type on a keyboard, other types of software can just as easily access and record film and audio footage from the microphone and camera on your PC or mobile phone.

2.3 (f) 'Bulk personal datasets'

The DRAFT Code notes that ' bulk personal dataset' refers to the practice of the Security and Intelligence agencies of collecting 'information from a variety of sources'[150] whereby the information collected contained 'personal data relating to a number of individuals.'[151] This personal data is then 'held on electronic systems for the purposes of analysis.'[152] There is little official information as to what types of information constitute 'personal information' as well as their potential sources. The MI5 provides two examples: the electoral roll, telephone directories or travel related data.[153] Big Brother Watch, the civil liberties and privacy pressure group, makes the addition of driving and vehicle licenses, credit reference agency information, land registry information, National Insurance numbers, Oyster card data and passenger name records and flight data.[154] There does seem to be the implications that 'bulk personal datasets' are not limited to the records of government agencies but also those of private companies, given that 'passenger name records and flight data' is noted as an example. Given that 'bulk person datasets' merely infers the collection of personal data, data freely published on websites (such as Facebook) may also be subject to a 'bulk personal dataset'.

Again, this provision does not strictly relate to the Internet or networked communications. That said, a lot of data included in the examples is collected,

---

[150] Home Office, 'DRAFT Code of Practice; Intelligence Services' Retention and Use of Bulk Personal Datasets', December 2016, pp.4, §2.1, (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/668933/Draft_BPD-_Intelligence_Services_Retention_and_Use_of_Bulk_Personal_Datasets.pdf)
[151] ibid. §2.2
[152] MI5, Bulk Data, (https://www.mi5.gov.uk/bulk-data)
[153] ibid.
[154] Big Brother Watch, Investigatory Powers Act Factsheet; Bulk Personal Datasets, (https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Bulk-Personal-Datasets.pdf)

nowadays, through online forms provided by the government and 3rd party websites. A decade ago, one would have had to fill out a paper form in order to apply for a driver's license or utilize telecommunications services etc. Thusly, I would not classify this as an example of 'internet surveillance' per se. Like 'equipment interference', it is an example of how the Internet is used to facilitate surveillance activities, which would instead constitute the active collection, storage and manual/automatic analysis of such information.

Despite the fact that 'equipment interference' and 'bulk personal datasets' are not types of internet surveillance in a strict sense, it is still important, for the purposes of this thesis, to consider them as falling within its ambit. This is due to the fact that the existence and usage of the Internet have allowed the government to utilize surveillance techniques on a scale and level of intrusiveness never seen before. This is to the degree that 'the internet' and older forms of surveillance (such as reading and analyzing government records of someone) cannot be logically separated. In order to see in more detail how the invention of the Internet has affected data surveillance, please review Chapter 1.4 (d).

2.3 (g) Targeted and Bulk Powers

Part 6 of IPA 2016 includes, what are known as, 'bulk powers'. These stipulate that, subject to particular circumstances, security agencies can engage intercept communications, acquire communications data and interfere with equipment when there is no particular target in mind (the mentioned powers listed in Parts 2 – 5 of the Act is conversely referred to as targeted powers). Data is acquired/intercepted on a large-scale and may include that of individuals that are of no particular interest to the security services. As well as providing for the circumstances in which data can be collected in bulk, Part 6 also includes provisions on when such data can be selected for examination. Bulk powers differ in terms of their geographical scope. Bulk acquisition of communications data cannot be imposed on ISPs, '…whose equipment is not in or controlled from the UK and who do not offer or provide services to persons in the UK.'[155]. On the other hand, bulk equipment interference, is limited to the acquisition of data from overseas and cannot be legally used on people '…in the British Islands.'[156] The same applies to bulk

[155] Home Office, 'DRAFT Code of Practice; Bulk Acquisition', Autumn 2016, pp.4, §2.2, (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557863?IP_Bill_-_Draft_Bulk_acquisition_code_of_practice.pdf)
[156] Op.cit. 'DRAFT Code; Equipment Interference', pp.66, §6.1,

interception, it being legally restricted to 'communications…sent or received by individuals outside the British Islands,'[157].

I have chosen to place 'bulk personal datasets' in a separate section (see above) because, unlike the other forms of surveillance, there is no targeted alternative. The very nature of a 'bulk personal dataset' is that data is harvested in large quantities, which may then be selected for examination or analysis as part of an investigation into an individual/individuals. Data selected for examination from a bulk personal dataset must be 'referable to an individual known to be in the British Islands at the time of selection.'[158]

2.3 (h) Levels of intrusiveness

As detailed, the IPA 2016 permits the use of a range of surveillance powers. The main question for the purposes of this thesis is; to what extent should these various powers be considered more or less intrusive? It stands to reason that, the more intrusive the power, the stricter the safeguards should be in order to prevent a potential breach of privacy rights. This question is fraught with subjectivity. Notwithstanding, the DRAFT Codes do provide some limited insight as to how the various powers are regarded. The DRAFT Code expressly states that content data (the written content of an email for example) is more 'intrusive' than communications data.[159] Moreover, it is also stated that communications data is a less broad form of secondary data (the definitions of which can be found above). This goes to suggest that powers enabling the acquisition of solely communications data are less intrusive than those enabling the acquisition of secondary data (this including both communications and other forms of data).

The DRAFT Codes do not provide commentary on whether bulk powers are intrinsically more intrusive than targeted powers. Prima facie, one would suggest that bulk powers are more intrusive by virtue of its comparatively indiscriminate approach to data collection. Then, again the data is collected in such large proportions that it would impossible to analyze it without targeting the specific data of interest. Are bulk powers necessarily more intrusive if most of the data is discarded without analysis? Another aspect of the comparative intrusiveness of bulk and targeted data relates to its geographical scope of application. As stated, all bulk powers can only be used overseas except for the 'bulk acquisition of

[157] Op.cit. 'DRAFT Code of Practice; Interception of Communications', pp.52, §6.1
[158] Op.cit. 'DRAFT Code of Practice;…Retention and Use of Bulk Personal Datasets', pp.13, §4.17
[159] See. Chapter 2.4(a)

communications'. In this sense, one could argue that the 'bulk acquisition of communications' is the least intrusive of the bulk powers; its usage being limited to the domestic population of the UK (numbering 65 million) as opposed to the population of the rest of the world. Conversely, from the perspective of the domestic population of the UK, 'bulk acquisition of communications' can be argued to be the most intrusive. This serves to highlight the subjective nature of the notion of intrusiveness.

Keeping the idea of intrusiveness in mind, the next chapter will detail the provisions of the IPA 2016 that serve to guard against the indiscriminate usage of the drafted surveillance powers. I will take a comparative approach, highlighting and commenting on how the safeguards vary between the powers and speculating as to the reasoning behind it. I will seek to answer the question of whether the relative strength of the safeguards have any bearing as to the relative intrusiveness of the powers.

2.4 Authorizations, judicial oversights, and safeguards provided for by the IPA 2016

A large proportion of the IPA 2016 consists of provisions limiting the use of surveillance powers by the security services and other government bodies. To use these powers, one must adhere to strict legal rules and satisfy judicial scrutiny. Once data is acquired, its usage is also subject to legislative and judicial safeguards. Acts of surveillance initiated outside the IPA 2016's prescribed mechanisms are without 'lawful authority' and those responsible can be subject to criminal prosecution. The penalty for a person found guilty of an offense under the Act is a fine and/or a prison sentence (for unlawfully obtaining communications data, one can receive a 12-month sentence maximum[160]).

Permissions, judicial oversights, and safeguards are the three main methods of preventing government bodies from using surveillance powers with impunity and having free reign over how the data is then used. They also serve to limit the bodies and individuals who are able to access these powers. This is where the IPA 2016 becomes very complicated.

My use of the word 'permission' refers to the process in which an individual or government body must defer to a higher authority when wanting to use a certain surveillance power. The higher authority will then grant permission, only if their

[160] Op.cit. IPA 2016, Part 1, Section 3, §4 & §6 (c)

proposed usage fulfills legislative criteria. This process is referred to by the IPA 2016 using the terms; warrants, authorizations, and notices. Despite being similar in the fact that they all involve the seeking and granting of permission to use a surveillance power, they do differ in meaning. I will explain how later in the thesis.

'Judicial oversights' refers to the powers afforded by legislation to an impartial judicial body to provide the final say as to whether 'permission' to use a power should be granted (i.e. the judicial approval of a warrant). This is crucial to ensure that such powers are not being used in an indiscriminate or unjust way. It also guards against the use of such powers for political means. It is important to analyze the extent to which the judiciary is integrated; do they have heavy involvement or light involvement? I will go on to look at how they are integrated into the IPA 2016.

'Safeguards' and 'restrictions' are general legislative rules that restrain and guide the usage of powers after permission has been sought and granted. If an individual or government body wishes to act in a way that breaches a safeguard, additional permissions may be sought or modifications may be made to the original permission. This may or may not require the involvement of a judicial body to approve it.

I will continue by looking at the types of permissions there are in the IPA 2016 for each power (Interception of communications, equipment inference etc.). As stated, these are referred to by the act as; warrants, authorizations, and notices.

2.5 (a) Permissions

2.5 (a)(i) Warrants

Government usage of **'**interception of communications', 'equipment interference' and 'bulk personal datasets' is unlawful unless permission has been granted by virtue of a warrant (albeit with some exceptions)[161]. There are numerous types of warrants for each power. For IOC there are 'targeted interception warrants'[162], 'bulk interception warrants'[163] and 'targeted examination warrants.'[164] EI warrants are organized in the same way. There are two types of warrants for BPDs: the 'class BPD warrant' and the 'specific BPD warrant'.[165]

[161] See. IPA 2016, Part 2, Chapter 12 for exception relating to 'interception of communications'
[162] IPA 2016, Part 2, Section 15(2)
[163] ibid. Section 15(4)
[164] ibid. Section 136
[165] ibid. Part 7, Section 184(3)

2.5 (a)(i)(i) IOC warrants

Types of warrant

'Targeted interception warrants' permit the 'person to whom it is addressed to intercept the communications described in the warrant and/or secondary data'[166]. As the name suggests, a 'bulk interception warrant' permits the same thing but on a bulk scale. The third type of warrant mentioned, the 'targeted examination warrant', serves as a corollary to the 'bulk interception warrant', it authorizing the selection of data obtained through 'bulk interception' for examination.

Who can apply?

The persons who can apply for 'targeted interception warrants' are listed in Part 2, Section 18(1) and generally include the most senior members of internal security and law enforcement (i.e. The Director General of the Security Service). These number nine in all. The only persons who do not strictly fit this remit are 'the Commissioners for Her Majesty's Revenue and Customs' (HMRC). The HMRC's main responsibilities are to administer the collection of tax and distribute social security payments. That said, the body is also involved in the prevention of crime, producing regulations relating to the prevention of money laundering.[167] The numbers of authorities that can apply for a 'bulk interception warrant' are severely reduced, it being restricted to the three most senior people of the security services.

The subject matter of warrants; thematic or non-thematic

'Targeted warrants' ('targeted interception warrants' and 'targeted examination warrants') must be drafted so as to 'specify or describe the factors used for identifying the communications to be intercepted or selection for examination.'[168] This includes 'addresses, numbers, apparatus, other factors' or a combination thereof.[169] Any factor specified must identify communications which 'are likely to be or include – (a) communications from, or intended for, any person or organization

[166] Op.cit. 'DRAFT Code of Practice; Interception of Communications', pp.14, §4.5
[167] HM Revenue and Customs, 'Money laundering supervision: introduction', 23 October 2014 (https://www.gov.uk/guidance/money-laundering-regulations-introduction)
[168] Op.cit. 'DRAFT Code of Practice; Interception of Communications', pp.20, §5.4
[169] Op.cit. IPA 2016, Part 2, Chapter 1, Section 31, §8(b)

named or described in the warrant, or (b) communications originating or, or intended for transmission to, any premises named or described in the warrant.'[170]

The three entities described in Section 31 – person, organization, and premises (the definitions of which can be found in Schedule 1 to the Interpretation Act 1978) – can be described by the warrant individually (i.e. Osama Bin Laden). Alternatively, the warrant can be drafted in such a way that encompasses numerous people, organizations, and premises in accordance with a specific 'theme'. An example of a 'theme' would be 'a group who shares a common purpose'[171] There must be a full and thorough description of the 'theme' as well as a list of every person/organization/premises that might be encompassed within it, as reasonably practicable. In cases where it is deemed not 'reasonably practicable' to describe in further detail, written justification must be provided.[172] These have been termed 'thematic' and 'non-thematic warrants'. 'Bulk interception warrants', conversely, are not required to name a person organization or set of premises – data being collected indiscriminately and *en mass*. Specificity is instead covered by the targeted-examination warrant, which is required to examine bulk data.

Format

An application for targeted-interception and targeted-examination warrants must be drafted in a specific format. The format - detailed by pages 30 and 31 of the DRAFT Code of Interception of Communications – consists of around 18 points, which go towards ensuring that the legal, operational and formal ramifications have been fully considered by the applicant before its submission. Points (a) of both types of warrant require the applicant to include information on:

…The statutory ground(s) on which the warrant is sought is considered necessary. Any application for a warrant in the interests of the economic well-being of the UK should identify how those interests are also relevant to the interests of national security…

Bulk interception warrants must also be formatted in a specific way, the details of which are covered by the aforementioned DRAFT code on page 56.

Authorization

[170] ibid. §9 (a) and (b)
[171] ibid. Part 2, Chapter 1, Section 17, §2
[172] Op.cit. 'DRAFT Code of Practice; Interception of Communications', pp.25, §5.15

Once any type of warrant application has been made by – or on behalf of - one of the listed authorities, it must be presented to the Secretary of State for consideration. It is the Secretary of State who has the power to either authorize or reject an application at first instance. Authorization can only be granted if the Secretary of State is satisfied that '…necessary for a legitimate purpose and proportionate to that purpose.'[173] This is otherwise referred to as 'necessity'. For targeted interception, 'legitimate purposes' include (a) the 'interests of national security'[174] (b) for 'the purposes of preventing or detecting serious crime'[175] or (c) 'in the interests of the economic well-being of the United Kingdom' as long as they are related to 'interests of national security.'[176] The latter purpose is only considered 'legitimate' if the data to be retrieved relates to 'acts or intentions of persons outside the British Islands'[177], thereby prohibiting the domestic use of interception in such circumstances.

Whereas for targeted interception warrants it is sufficient for the legitimate aim to be (a), (b) or (c), bulk interception warrants and targeted examination warrants must always have (a) - national security - at its core.[178] The reason for this relates to the fact that the warrants can only be used to retrieve and examine exterritorial communications. Indeed, to prevent or detect serious crime in another country would be beyond the remit of the UK's Security Services.

One a 'legitimate purpose' has been identified; The Secretary of State must then apply the test of 'proportionality' to the proposed conduct. As stated by the DRAFT code, 'any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy…against the need for the activity…'[179] to bring about a 'realistic prospect' of achieving its purpose. The conduct would be disproportionate/arbitrary if the same outcome could be achieved through a less intrusive means (i.e. intercepting secondary data instead of communications). The Secretary of State must also consider is to what extent the proposed conduct serves/is a detriment to the 'public interest'. Compliance with Human Rights[180], the 'integrity and security of telecommunications systems'[181] and the 'sensitivity'[182] of the data in

[173] ibid. pp.16, §4.10
[174] IPA 2016, Part 2, Chapter 1, Section 20, §2(a)
[175] ibid. §2(b)
[176] ibid. §2(c)
[177] ibid. §4
[178] ibid. Part 6, Chapter 1, Section 138, §1(b)(i)
[179] Op.cit. 'DRAFT Code; Interception of Communications', pp.17, §4.12
[180] IPA 2016, Part 1, §4(d)
[181] ibid. §2(c)
[182] ibid. §2(b)

question are noted as being related to this. Other guidelines related to the application of the test are published in IPA 2016, Part 1, §2(2). Concerning thematic warrants, The Secretary of State must be satisfied that the 'theme' has been adequately fleshed-out so as to fulfill the requirements of Section 31.

2.5(a)(i)(ii) EI warrants

Types of warrant

There are three types of EI warrant; 1) targeted-equipment interference warrants 2) targeted-examination warrants and 3) bulk-equipment interference warrants. Listed in sections 99(1), 99(2) and 99(9) respectively, these warrants are barely distinguishable from their IOC counterparts (see above for a full description). Indeed, the only functional difference between IOC and EI warrants lies in the surveillance methods they permit. One cannot perform acts of interception with an EI warrant, despite the fact that the types of data that might be obtained through such methods could be the same (communications and secondary data – including equipment data). EI and IOC are distinct acts and must be considered separately.

One notable difference between the law applicable to EI and IOC lies in the fact that it is not mandatory for the security services to obtain equipment interference warrants in cases when a) a CMA (Computer Misuse Act 1990) offense would not be committed b) there is no British Islands connection.[183] Notwithstanding, if the Security Services are able to obtain a warrant, it is recommended that they do.[184]

Who can apply?

The number of officials who can apply for a targeted equipment interference warrant is more than double the number of officials who can apply for a targeted interception of communications warrant. Not only does it include the most senior officials of the Security Services and law enforcement, it also lists the most senior officials of the military police, senior immigration and customs officials (if specifically designated by the Secretary of State), senior officials of the HMRC (if specifically designated by the HMRC), the chair of the Competitions and Markets Authority and the most senior officials of the bodies responsible for reviews, investigations and complaints into the Police.[185]

[183] Op.cit. 'DRAFT Code; Equipment Interference', pp.17, §3.31
[184] ibid. pp.15, §3.25
[185] Op.cit. IPA 2016, Part 5, Sections 102, 104 & 106

Like the IOC, the number of people who are able to apply for a targeted equipment examination warrant and a bulk equipment interference warrant is drastically reduced, they being limited to the most senior members of the Security Services (i.e. the Director of the GCHQ).[186]

Unlike with IOC, the Secretary of State is not the only issuing authority in the case of targeted equipment interference warrants and targeted examination warrants. In cases where an application is made by an 'appropriate law enforcement officer' of the listed 'law enforcement agencies', warrants can be considered and issued by a 'law enforcement chief.'[187]

The subject matter of warrants; thematic or non-thematic

Like with IOC, targeted equipment interference warrants and targeted examination warrants can either be thematic or non-thematic in nature and largely takes on the same form. Non-thematic warrants will target particular pieces of equipment that belongs to, is used by or in the possession of a particular person or organization. It can also be used to target a piece of equipment in a specific location.[188] In cases where there is an interest in multiple pieces of equipment, it is necessary to define the theme that links them (i.e. there is a common purpose or shared activity between the people that the equipment belongs to).[189] Like with IOCs, the theme must be fully fleshed-out and there must be specificity as to the target where 'reasonably practicable'.[190]

Format

EI warrant applications (targeted, bulk and targeted examination) to be valid, must be drafted in strict accordance with the numerous stipulated formats. These are outlined on pages 37 – 45 of the DRAFT Code. These ensure that the specific details and 'themes' of the applications are adequately 'fleshed out' and that ramifications concerning 'legitimate aim' and 'proportionality' have been explored. The formatting also ensures that the applications are being made by/on behalf of an authority who had the right to do so.

Authority

[186] Op.cit. 'DRAFT Code; Equipment Interference', pp.22, §4.6
[187] ibid. pp.28, §5.6
[188] ibid. pp.29, §5.8
[189] ibid. pp.31, §5.12
[190] ibid. pp.32, §5.15

The Secretary of State (and, in certain cases, a chief law enforcement officer), before issuing a warrant, must consider whether the planned course of action has a 'legitimate aim' and fulfills the doctrine of 'proportionality'. This is conducted in much the same way for all types of warrant (See above. For further detail).

2.5(a) (i) (iii) Bulk Personal Datasets

Types of warrant

There are two types of BPD warrant available under the IPA 2016; (a) 'class BPD warrant' and (b) 'specific BPD warrant'.[191] Whereas the former warrant permits the applying authority to retain and/or examine any PD (personal dataset) falling within a specific 'class' (i.e. travel dataset), the latter type of warrant will be utilized where the PD sought does not fall – or easily fit - into a particular 'class' of BPD. Given that most PDs do fit into a 'class' of BPD, a specific warrant will only be applied for in rare cases. Other reasons for applying for a specific BPD might include the associated political ramifications of retaining and examining the dataset in question, as well other consideration.[192]

As highlighted by my use of and/or, warrants of either kind can permit the applicant to either retain a PD or retain and examine a PD. Where an applicant is permitted only to retain a PD, he cannot also examine that data without modifying or applying for a new warrant.

It is possible to obtain BPDs through other types of warrants. In these cases, the stipulations of Part 7 do not apply. A BPD, for example, might be obtained through acts of bulk/targeted interception of communications or equipment interference (either on purpose or inadvertently). An example provided by the DRAFT code is; 'where an email had been intercepted and a BPD was attached to the email'.[193]

Who can apply?

Class and specific BPD warrants can be only made by – or on behalf of – the most senior members of the security services.

The subject matter of warrants; Class and specific BPD warrants

[191] Op.cit IPA 2016, Part 7, Section 204 - 205
[192] Op.cit. 'DRAFT Code of Practice;…Retention and Use of Bulk Personal Datasets', pp14, §4.23
[193] ibid. pp.12, §4.11

In terms of class datasets, the applying authority is not free to retain or examine datasets of any class of their choosing. Section 202 of the IPA 2016 restricts the choice of certain class datasets if the:

Head of intelligence considers that: (a) the BPD consists of, or includes, protected data; (b) the BPD consists of, or includes, health records; (c) a substantial proportion of the BPD consists of sensitive personal data; or (d) the nature of the BPD, or the circumstances in which it was created, raises novel or contentious issues…[194]

These 'novel or contentious issues' must be considered before the Secretary of State before the warrant can progress.

'Health records' are self-explanatory although further detail can be found in Section 206(6) of the IPA 2016. 'Protected data' refers to identifying data and systems data, both of which have been described earlier in the thesis. 'Sensitive personal data' refers to such forms of data 'consisting of information as to – (a) the racial or ethnic origin of the data subject (b) his political opinions (c) his religious beliefs…' etc.[195]

This rule also applies if the BPDs contains confidential information relating to members of a 'sensitive profession'. Sensitive professions are outlined as 'lawyers, doctors and journalists' and confidential information would include such things as correspondence between the professional and their client.[196]

Where such circumstances materialize, the applying authority must instead opt for a 'specific warrant'.

Format

Like with other types of warrant, the class BPD warrant must elicit the type of data to be found which – in this case – necessitates a description of the BPD and a description of what 'class' the BPD can be categorized as. It must also include an assessment as to any privacy risks (E.g. Does the BPD contain any confidential information relating to a sensitive profession?) and whether the level of intrusion is necessary/proportional.

Where a specific warrant is concerned, the warrant must go into further detail into the 'nature and scope of the BPD'[197], given the fact that the applicant cannot make reference to a specific 'class'. The applicant, must however

[194] ibid.
[195] Data Protection Act 1998, Part 1, Section 2 (a) – (c)
[196] Op.cit. DRAFT Code; ..Retention and Use of BPD, pp.13, §4.14 – 4.17
[197] ibid. pp.19

also make efforts to explain as to what type of categories, if any, the BPD in question can fit into. Given that specific warrants will often be applied for on the basis that the BPD will contain sensitive information or protected data, the warrant will need to contain a description of the 'nature and extent' of such data[198] as well as to what the source pertains (e-mails, letters etc.)

Authority

BPD warrants can only be issued by the Secretary of State. As per usual, he is required to apply the doctrine of necessity and proportionality (See. Above) and only permits the acquisition, examination, and retention of BPDs where the same aim cannot be accomplished through a less intrusive means.

2.5(a)(ii) Authorizations

There is one surveillance power under the IPA 2016 whose permission is termed an 'authorization' instead of a 'warrant', listed in Part 3 as 'authorizations for obtaining communications data'. That said, I will also be considering another type of 'warrant' under this section. This is by virtue of the fact that only permissions for the targeted obtaining of communications data are termed as authorizations. Bulk acquisitions (the power to obtain communications data in bulk), on the other hand, are referred to as warrants. This is found in Part 6 Chapter 2 of the IPA 2016. Instead of examining this power in the 'warrant' section above, for the sake of clarity, I feel it is best to keep targeted and bulk powers of the same variety - the obtaining and examining of communications data - together.

2.5(a)(ii)(i) Authorizations for obtaining communications data

Types of authorizations

There is only one type of 'authorization' and it grants permission for an individual to acquire/obtain communications data. Authorizations do not permit acts of 'equipment interference' or 'interception'. Neither should it be used where the data in question is unlikely to constitute 'communications data'.[199] As said, an 'authorization' merely gives permission for the applicant to compel an ISP to provide the desired data. As such, it usually requires the ISPs active cooperation. That said,

[198] ibid.
[199] Home Office, 'DRAFT Code; Communications Data', Autumn 2016, pp.25, §5.6, (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557862/IP_Bill_-_Draft_CD_code_of _practice.pdf)

where the ISP is 'not capable of obtaining or disclosing the communications data', the applicant may still be able to acquire it so long as their actions in doing so cannot be classified as 'interception' or 'interference'.[200]

Who can apply?

A 'member of the public authority'[201] can apply for an authorization. The member in question (hereby referred to as 'the applicant') must be a person 'involved in conducting an investigation for a relevant public authority.' [202]

The Act's interpretation of 'public authority' is comparatively expansive and includes a large number of government agencies that cannot be said to constitute either the police or security services. Some examples are The Department of Health, the HMRC, the Department for Transport, the Department for Work and Pensions, The Financial Conduct Authority, the Food Standards Agency, the Gambling Commission and numerous others.[203] In comparison to the surveillance powers that I have already covered in this section (Interception of Communications, Bulk Person Datasets etc.), many more agencies have been permitted access to this particular power under the Act. As to why this is the case, I will discuss later in the thesis.

As far as can be taken from the words of the Act and the relevant DRAFT Code, 'a member' refers to anyone working within the organizations listed in Schedule 4 and makes no reference to the seniority or the level of authority that the applicant must possess.

The subject matter of authorizations

Applications must describe the 'communications data required' which includes whether the data in question 'relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation.'[204] The applicant must also specify the dates (past or future) or time periods from which he wishes to obtain communications data [205] (i.e. all communications data relating to the witness from 1st Jan 2018 – 1st Feb 2018). The Act does not differentiate between thematic or non-thematic authorizations, as mentioned before. Indeed, the level of 'specificity' required in applications for

[200] ibid. pp.34, §50
[201] ibid. pp.25, §4.2
[202] ibid. pp.26, §4.7
[203] Op.cit IPA 2016, Schedule 4, Part 1
[204] Op.cit. 'DRAFT Code of Practice; Communications Data', pp.26, §4.9
[205] ibid.

authorizations seems to be much lower than that of warrants. That said, whether the application is indeed too broad and unspecific is something that will be judged in the application of the test of proportionality.

Format

Applications must typically be submitted in a hand-written or electronic form. Applications can also be made orally in urgent circumstances (something that I will look a later).[206] A description of the communications data required, as mentioned above, must be provided. It must also include a full explanation of why the acquirement of data listed should be considered 'necessary and proportionate to what is sought to be achieved…' and a consideration of any 'unintended consequences'.[207] A final consideration is whether the ISP subject to the application is permitted to inform the customer that their data is in the course of being acquired by the government.[208]

Authority

Unlike warrants, authorizations are not required to be issued by the Secretary of State. Instead, they can be issued by a 'designated senior officer'. Those individuals that can be considered a 'designated senior officer' for the purposes of issuing an authorization are found in Schedule 4 of the IPA 2016. They typically occupy the most senior position of their respective 'public authority' (i.e. The Senior Manager of the Gambling Commission). For some government agencies, the second-highest ranking individual can also grant authorizations such as the Inspector of the Metropolitan police force – the Superintendent is the highest ranking.

Like warrants, authorizations may be granted if the 'designated senior officer' deems the proposed action to be a proportionate response to a legitimate aim (the tests of 'proportionality' and 'necessity'). The list of legitimate aims – found in section 61 of the Act - include the same as those relating to warrants: 7(a) the 'interests of national security', 7(b) for 'the purposes of preventing or detecting serious crime' and 7(c) 'in the interests of the economic well-being of the United Kingdom' as long as they are related to 'interests of national security.' That said, there are some additional aims that have not been drafted in relation to warrants such as: 7(d) in the 'interests of public safety' 7(e) 'for the purpose of protecting public

[206] ibid. pp.26, §4.7
[207] ibid. §4.9
[208] ibid.

health' and 7(f) 'for the purposes of preventing death or injury or any damage to a person's physical or mental health.' The list of 'legitimate aims' number ten in all.

One can see a clear link between the drafting of these additional legitimate aims and the drafting of additional government agencies in Schedule 4, who are capable of applying for/granting an authorization. For example, the 'purpose of protecting public health' would be an aim of particular relevance to the remit of The Department of Health.

Pursuant to Schedule 4, certain designated senior officers are limited in their power to grant authorizations. The limitations vary according to the specific agency and position of the designated senior officer and are related to the aforementioned 'aims' listed in Section 61. For example, the Inspector of the Metropolitan Police Force is able to grant authorizations as long as they purport to fulfill any of the Section 61 aims (7(a) – (j)). The Senior Manager of the Gambling Commission, on the other hand, can only grant authorizations so long as the application only purports to fulfill aim 7(b) of Section 61 which is: 'for the purpose of preventing or detecting crime or of preventing disorder.' It is evident that this has been drafted so as to prevent the agencies from overstepping their operational remit.

Furthermore, a designated senior officer may also be prohibited from granting authorization where they concern the acquisition of a certain form of data. According to Schedule 7, the Inspector of the City of London Police force may only grant authorizations where it concerns 'entity data' (as a type of 'communications data') specifically. The Superintendent, on the other hand, may grant authorizations for all forms of data.

2.5(a)(ii)(ii) Bulk acquisition warrants (communications data)

Bulk Acquisition warrants operate in much the same way as the bulk warrants considered above, including the way in which they can only be used to acquire data concerning targets who are outside the British Isles. The warrants can only be used to acquire communications data and any action that is considered interception or interference under the Act must only be done in accordance with a Bulk interception/interference warrant. Only the most senior members of the security services can apply for the warrant, with the warrant being issued by the Secretary of State after applications of the tests of legitimate aim and proportionality (See. Home Office, DRAFT Code of Practice; Bulk acquisition of Communications Data, December 2016 and section 2.5(a)(ii) – 2.5(a)(iii) of this thesis).

2.5(a)(iii) Notices

'Notices' functionally differ from authorizations and warrants. Whereas warrants and authorization grants permission to the applicant to engage in certain acts (i.e. interception of communications) in order to acquire certain forms of data (i.e. systems data) and fulfil a predetermined aim, notices are served to ISPs in order to compel their cooperation with an investigation and may require them to take certain actions. Due to the nature of notices, they only apply to those 'who offer or provide a telecommunications service to persons in the UK or provides a telecommunications system which is (wholly or in part) in or controlled from the UK.'[209]

Notices cannot be used in situations that would require a warrant or an authorization such as the interception of communications data.

Types of notice

There are four types of 'notice' provided for by the Act. The first relates to the acquisition of communications data discussed above and is covered by Part 3, Sections 64 – 65 of the Act. These are used in conjunction with authorizations in order acquire communications data. Where an authorization has been granted to a member of the public authority to acquire certain communications data, it may be necessary to serve an ISP with a notice in order to facilitate the acquisition. In many cases, the ISPs will already possess the communications data in question. Where they do not have the data, they will certainly have the capabilities to acquire it on behalf of the public authority.

The second type are known as 'retention notices' and are contained in Part 4 of the Act. These are issued by the Secretary of State to 'a particular operator or any description of operators' and can require that operator to retain all or some communications data of a certain description for a certain time period, not exceeding 12 months. [210] These are also used in conjunction with the acquisition of communications data.

The third is termed a 'National Security Notice' which is covered by Part 9, Sections 249, 252, 254 and 258 of the Act. This allows the 'Secretary of State to give a notice to a telecommunications operator in the UK requiring the taking of specified

[209] Home Office, 'DRAFT Code of Practice; National Security Notices', December 2017, pp.3, §2.4, (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/668939/Draft_code_-_National_Security_Notices.pdf) _
[210] IPA 2016, Part 4, Section 87 (2)(a) – (c)

steps' that he/she 'considers necessary in the interests of national security.' What 'specified steps' means is not strictly stipulated, although some vague examples are provided by the DRAFT Code such as: 'to carry out any conduct for the purpose of facilitating done by an intelligence service; to carry out any conduct for the purpose of dealing with an emergency' etc.

The fourth is known as a 'Technical capability Notice' and is found in Part 9, Section 253. It is similar to a 'National Security notice' and is issued where 'the Secretary of State considers that the notice is necessary for securing that the operator has the capability to provide any assistance which the operator may be required to provide in relation to any relevant authorization.'(IPA 2016, Part9, Chapter 1, Section 253).

For the purposes of this thesis, I will be focusing on notices in relation to 'authorizations' as well as 'data retention notices'. This is due to the fact that they are the only types of notice that have direct implications for the data – more specifically, the communications data - of private citizens. 'Technical capability notices' and 'national security notices' require ISPs to act in accordance with the directions of the Secretary of State, but makes no reference to data per se.

Who can apply?

In relation to acquiring communications data through authorizations – considered above – a 'member of the public authority' can apply for the issuing of a notice as part and parcel of an application for an authorization. The list of 'public authorities' or who are eligible to make an application are listed in Schedule 4 of the Act.

For 'retention notices', it is stated that 'key operational agencies (including law enforcement agencies and security and intelligence agencies) maintain governance arrangements in order to identify operational requirements, including the potential requirement to issue a data retention notice.'[211] As such, applications are not made by a government agency in the traditional sense. Government agencies – as stated - merely 'identify an operational requirement' for communications data to be retained by the ISP. This requirement is then noted by the Home Office who, in collaboration with the ISPs and the Secretary of State, take more formal steps towards the drafting and issuing of the notice.

[211] Op.cit, 'DRAFT Code; Communications Data', pp.84, §14.1

The subject matter/format of notices and authority to issue

I have decided to combine the above stages, given that the process for issuing an 'authorization' notice and a retention notice are not as clearly/formally defined or extensive.

To issue an ISP with a retention notice, there is no formal applications process that must occur beforehand. It is merely up to the discretion of the Secretary of State (and the Home Office), after taking into account numerous factors and considering it as necessary and proportional to do so. This will include a period in which the Home Office and the Secretary of State will directly engage with ISPs that might be affected. Concerns, technical issues as well as what the ISP will be required to do if a retention notice is issued will be discussed. Throughout these discussions, the Secretary of State is required to bear in mind; 'the size of the CSP…the speed of growth of the CSP…whether the CSP operates a niche service.' Etc.[212] It will help him/her come to a decision on the question of 'necessity'. Factors that the Secretary of State will have to take into account when considering 'proportionality' must include such things as: 'The likely benefit of the notice – the extent to which the data to be retained may be of use to the public authorities…The likely number of users of the services to be covered by the notice – this will help the Secretary of State to consider...the level of intrusion on customers.'[213] The DRAFT Code lists several other issues for consideration. The 'retention notice' may be issued if the Secretary of State is satisfied that it is 'necessary and proportional.'

Where a 'member of the public authority' seeks a notice in order to acquire specific communications data, once a designated senior officer has provided an 'authorization to acquire communications data' – outlined above – he must then draft the notice and then serve it to the relevant ISP. The notice must be drafted in a specific fashion and include the information listed in §4.71, pp. 37 of the DRAFT Code; Communications Data, which includes such things as a description of 'the communications data to be obtained or disclosed…' a specification of 'the requirements being imposed and the telecommunications operator on whom the requirements are being imposed…' and 'an indication of any urgency or time within which the CSP (ISP) is requested to comply with the requirements of the notice…', among others.

2.5(b) Judicial Oversights

[212] ibid. pp.84, §14.3
[213] ibid. pp.86, §14.17

The IPA 2016 prevents the politicization of surveillance powers through the integration of 'independent' judicial bodies. The degree of their representation is not consistent throughout the Act and they vary in their role from surveillance power to surveillance power. This will be the focus of the section.

According to the IPA 2016, there are two judicial bodies of whom serve to mediate the government's use of the surveillance powers contained; the Judicial Commission (JC) and the Investigatory Powers Commission (IPC). Unlike the former, the latter body is composed of just one individual.

It is the duty of the Prime Minister to appoint people to these positions albeit – in the case of the IPC - with the 'joint recommendation from the Lord Chief Justice of England and Wales, the Lord President of Scotland, the Lord Chief Justice of Northern Ireland and the Lord Chancellor'[214]. No-one may be appointed as the IPC or as a member of the JC unless they have held a judicial position to the equivalent seniority of a High Court judge.'[215]

The JC and IPC must ensure that the government's usage of the IPA 2016's surveillance powers are necessary and proportional, and can refuse approval if not. The Act makes clear that this function requires an application of 'the same principles that a court would apply on an application for Judicial Review.'[216] This makes sense, given that, what the JCs and IPCs are essentially deciding on whether the powers are being utilized ultra vires. The principles themselves are the culmination of hundreds of years' worth of common law jurisprudence, and it is beyond the scope of this thesis to go into them in any great detail.

The JCs and the IC are provided with all the assistance and documentation that they may need to perform their job effectively, including access to the technical systems involved.[217]

Warrants

After a warrant has been issued by the Secretary of State (this includes all bulk/targeted warrants under the IPA 2016), the warrant must receive the approval of the 'Judicial Commissioners' (JCs).

The 'Judicial Commissioners' must conduct a thorough review of the warrant with respect to the test of necessity and proportionality. In the event that the warrant is rejected by the JCs, the applying agency may re-draft the application in

[214] ibid.
[215] Op.cit. 'Explanatory Notes', §107, pp.23
[216] ibid. pp.20., §84
[217] Op.cit. IPA 2016, Part 8, Chapter 1, Section 235

line with the JCs recommendations, whereby the Secretary of State can resubmit. An alternative avenue is to appeal the decision to the IPC, who will then consider the warrant along the same lines. In the event of another rejection, there are no further avenues for appeal, with the warrant remaining invalid.

Authorizations

Authorizations granted by a designated senior officer of a public authority to acquire communications data[218], neither require the approval of the JC nor the IPC. Instead, the authorization need only receive approval from the 'relevant judicial authority.'[219] The 'relevant judicial authority' is taken by the Act to mean 'a justice of the peace'[220]. Unlike with warrants, authorizations not require approval from a senior judge. Instead, any judge is able to approve an authorization. Where the 'justice of peace' believes that the authorization fails to fulfill the standards necessity and proportionality, he/she can make 'an order quashing the authorization.'[221]

Notices

Retention Notices must be reviewed by the JC and the IPC in much the same way as warrants.[222]

Given that the authorization for acquiring communications data has been approved by a 'justice of the peace' (See. Above), a notice that is drafted by the senior designated officer in order to give effect to the authorization need not acquire any additional judicial approval before it can have an effect.[223]

2.5(c) Restrictions and Safeguards

Thus far, I have described how the IPA 2016 restricts the unbridled usage of the surveillance powers contained through a 'permission' system (in the form of a warrant, authorization or notice) and through allowing for judicial oversight. These are the hurdles the government must jump before acts of interception or equipment interference etc. can legally be committed. Notwithstanding, the government is still restricted in terms of what they are able to do and how long they are able to do it,

[218] See. IPA 2016, Part 3, Section 75
[219] ibid. IPA 2016, Part 3, Section 75(7)
[220] ibid. 7(a)
[221] ibid. Section 75(6)
[222] ibid. Part 4, Section 89
[223] ibid. IPA 2016, Part 3

during and after the power has been granted. This is by virtue of a number of provisions, which I am terming as 'restrictions' and 'safeguards.'

By 'restrictions', I am referring to the warrant/authorization/notice itself and the IPA 2016 provisions related to their duration, cancellation, renewal, and modification. Once a permission is issued, its integrity is protected and the government must fulfill the additional requirement in order to change it. I am using the term 'safeguards' in the same way as the IPA 2016, this referring to provisions affect the government ability to retain and disclose data that has been acquired through a surveillance power, as well as its destruction.

With reference to 'restrictions', the IPA 2016 treats the modification or renewal of an existing warrant/authorization/notice as if it was being newly created. In the case of warrants, the Secretary of State possessed the power of modifying or renewing warrants, this being overseen by the JC and the IC. At every stage, the test of necessity and proportionality must be applied. Where these tests are not satisfied, the modification will be denied or the warrant will be canceled. Warrants/authorizations/notices are only valid for a certain duration, after which, they must be renewed. Where there is no renewal, they are automatically canceled.

Concerning 'safeguards', the government is restricted to using the data obtained in a way that is necessary and proportional. Such safeguards affect; 'the number of persons to whom the material is disclosed…the extent to which the material is copied…the number of copies that are made' Etc. Ergo. The government can only produce 100 copies of the material obtained if it is considered necessary and proportionate.

The restrictions and safeguards drafted in the IPA 2016 are subject to high degrees of nuance between the powers and delineating all the differences would be beyond the scope of this thesis. I believe that it is merely important to note their existence as well as the fact that the test of 'necessity and proportionality' is woven into the fabric of the Act, consistently mediating the usage of the powers contained.

2.5 (d) Overview of Chapter 2.5

The IPA 2016 is a piece of legislation that is over three-hundred pages long, replete with long, complicated lists of provisions and jargon. The purpose of this section was to provide a brief overview of the Act, that serves to highlight the ways in which it legislates for and responds to alternate surveillance powers with – arguably – alternate levels of 'intrusiveness.' In doing so, I attempted to avoid being

inundated with the technicalities so as to provide a clear and concise context for the following sections. I urge you to find and inspect Act itself for further information.

I will continue by providing a commentary on the Act's provisions, including further discussion on whether the Act attempts to account for varying levels of intrusiveness via a sensitive and nuanced approach/applications of the permissions procedures, judicial oversights and restrictions/safeguards.

.

2.6 Commentary

The problem of thematic warrants

'Thematic warrants' featured in relation to 'equipment interference warrants', this being something that has received a relatively large degree of public attention and disapproval. Criticisms concern the fact that 'thematic warrants' seem not negate the requirement to identify 'each target of the surveillance to be identified in the warrant.'[224] Its opponents deem it to be far too general and ill-defined, possibly leading to abuse. It has been highlighted, in arguments to this effect, that there are no provisions requiring that individuals or premises be subject to a degree of 'suspicion' as to their involvement in criminal (or other activities) before they can be caught by the warrant.[225] It merely requires there to be a past or present 'connection', something which I detailed in the section on 'equipment interference warrants', on page 33.

The advocacy group Liberty, states that its open-ended nature could result in 'wide-sweeping powers' interfering with the rights of 'hundreds or thousands of people' in the course of a single investigation[226]. It is curious why 'thematic warrants' only formed part of equipment interference and not interception of communications.

Lack of Judicial oversight for warrants (The JCs and the IPC)

Another aspect of the IPA 2016 that has been subject to criticism is the supposed lack of judicial oversight in regard to the application and issuing of warrants. This was something that numerous Parliamentarians commented upon in

[224] Camilla Graham Wood, Thematic warrants: 'Destroying democracy under the cloak of defending it'(2016), Solicitors Journal (https://www.solicitorsjournal.com/comment/thematic-warrants-destroying-democracy-under-cloak-defending-it)
[225] ibid.
[226] ibid.

the debates preceding the draft Bill[227]. It was also an argument put forward by Tom Hickman QC, co-opting the words of Lord Mansfield in the old case Leah v. Money[228]: "It is not fit that the receiving or judging of the information should be left to the discretion of the officer. The magistrate ought to judge."

It is indeed true that the power to issue warrants does lie with a member of the government, namely the Secretary of State, to which he must apply the tests of necessity and proportionality. Given this fact, it is obvious why there is concern over judicial oversight, given that it is imperative to the rule of law that such interferences of the rights of the individual should be mixed up with political considerations. The value of these criticisms is lessened, however, when one considers the safeguards put in place. A central part of the IPA 2016's warrant system is that the warrant is subsequently authorized by the JCs. As noted in Chapter 2.1(4)(a) of this thesis, the JC can only be composed of those who have held a judicial position at least as senior as a high court judge. The JCs are also required to apply the test of necessity and proportionality in their consideration of the warrant and treat the court procedure as if it were an instance of judicial review. Moreover, there is an appeal process resembling standard court procedure, the Secretary of State then being able to take the warrant to the IPC. This certainly seems to suggest a strong 'judicial oversight', contrary to the criticism levied against it. Of course, the judiciary can never be completely free from politics. Similar to the manner in which the highest court officials are selected, the JC and the IPC is composed of candidates selected by the Prime Minister, albeit with the mandatory approval of a number of legal officials including the Lord Chief Justice.

Purposes required for authorization & the list of bodies that can make authorizations (Schedule 4)

Section 61 § 7 of the IPA 2016 permits a large number of bodies to grant authorizations, enabling the applicant to access and examine communications data. Moreover, the purposes for which these authorizations can be granted are also quite numerous (see. Chapter 2 (a) (ii) of this thesis.) Warrants, on the other hand, are limited to situations that concern the interests of national security, preventing or detecting a serious crime and the interests of the economic well-being of the United Kingdom. Even though these categories are quite broad it would, arguably, be a

[227] Baroness Jones of Moulsecombe, 'Data Retention and the Investigatory Powers Bill, House of Commons Debate', 15.07.2014, Column 319
[228] Leah v. Money (1975) 97 Eng. Rep. 1075

difficult feat of reasoning to include some of the purposes included in Section 61 § 7 within their ambit. The reason why the drafting of the Act sees fit to include such a broad and comprehensive list of purposes is worthy of note and consideration, given that it could potentially lead to the abuse of such powers, enabling access to communications data in situations that, arguably, should not lead to such surveillance measures. One could hazard the question of whether the difference in the nature of the communications data and communications themselves (the former being debatably more intrusive than the latter) has resulted in this difference

Lack of judicial oversight for authorizations but not for warrants

Whereas data retention notices and warrants require the approval of the JC before they come into force, it is not the same for authorizations to access communications data. The decision is completely up to the 'senior officer of a public relevant public authority' to grant the authorization. This omission could be explained by the fact that the JCs are involved in the course of issuing data retention notices to ISPs with the ISPs, of course, being the sources of the communications data. Notwithstanding, it seems peculiar that the safeguard surrounding the granting of authorizations is so comparatively weak. Similar to what I said before, perhaps the reason for this difference lies in the perception of intrusiveness, with communications data (it being a form of secondary data) not being considered as sensitive.

Bulk interception warrants, bulk interference warrants, and bulk authorizations

I did not go into detail on bulk warrant and authorizations given the similarity of the provisions with their targeted counterparts. However, therein lies the criticism. Even though they include the tests of necessity and proportionality, given the sheer volume of data involved, some question whether such warrants could ever be considered necessary and proportional. Notwithstanding, criticisms concerning necessity have also questioned the efficacy of collection such large amounts of data[229]; whether it is indeed necessary to prevent crime and protect

[229] Liberty, 'Liberty's briefing on Part 6 of the Investigatory Powers Bill for Committee Stage in the House of Commons', April 2016 (https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%27s%20Briefing%20on%20Part%206%20of%20the%20Investigatory%20Powers%20Bill%20for%20Committee%20Stage%20in%20the%20House%20of%20Commons.pdf)

national security. Bulk powers can also be viewed as being too intrusive to fulfill the test of proportionality, with some speculating that:

> …The collection of vast volumes of data enables the identification of patterns and predictions of future behavior, a process called predictive analytics, data mining or Big Data. An example of this technique is a predictive policing system called PredPol, which analyses large volumes of crime reports to identify areas with high probabilities for certain types of crime.[230]

The problem with themed warrants

Warrants on targeted equipment interference have been viewed as problematic due to their inclusion of 'themed warrants'. Bulk warrants and authorizations can be viewed as suffering from the same problem in this regard. Bulk warrants essentially enable the potential for the personal data of many individuals unrelated to the investigation, to have their communications and secondary data be subject to collection, examination, and analysis.

The necessity and proportionality test's lack of direction

The terms necessity and proportionality are used frequently throughout the Parts on warrants, notices, and authorizations. However, I regard the lack of any theoretical indication (by way of the Explanatory Notes) or legal procedure as to how the test should be practically applied to be a notable omission given the complex nature of the situations that the Secretary of State or - in the case of authorizations - a senior legal official may be confronted with. That is not to say that the Secretary of State is mentally ill-equipped to deal with complex and critical scenarios, but the vagueness and subjectivity of the terms could arguably leave them open to abuse. Although it would be an extensive and extremely hard feat of legal drafting to accomplish; if such the test was elaborated on with some precision by the Act (possibly by way of a non-exhaustive list of potential scenarios), there would be a firmer legal basis from which to dispute them. That is not to say that necessity and proportionality are vague as part of English legal culture. Indeed, there is a massive common-law legal corpus dealing with precisely this issue, concerning every conceivable legal discipline. That said, we must realize that the Secretary of State is not a legal mind, and probably not in the best position to make such assessments.

[230] Op.cit. David Anderson QC, 'A Question of Trust', §4.40

Notwithstanding, this issue is almost entirely mitigated by the fact that any warrant decision made by the Secretary of State must receive approval by the JCs who are trained legal professionals and, as mentioned, apply the tests typical of an instance of Judicial Review. All that leaves is the authorizations, which as discussed, don't require any such approvals, and it is on this fact that I move onto the next matter.

Lack of judicial oversight for authorizations but not for notices

This is something I find particularly peculiar, given what each of these allows in terms of surveillance. As discussed, notices do not allow government agencies to access communications data from ISPs; it merely orders them to retain connection records for a maximum of 12 months. Authorizations, however, allow numerous employees from numerous government agencies to access and examination of connections data. Given this very fact alone, the expectation that authorizations should require a greater level of legal safeguards than notices is not an unreasonable one. Indeed, the only situation in which the JC are required to approve an authorization is in contained in Part 3, section 77: "Commissioner Approval for authorizations to identify or confirm journalistic sources." For me, it is this omission alone that is the most poses the most obvious threat to conceptions of privacy.

Interference & Interception; is specificity important?

In Chapter 1.3(5) I detailed some ways in which one could effectuate acts of, what the IPA 2016 refers to as, interception and equipment interference. These vague terms are not unique to the IPA 2016 are, as the ECtHR jurisprudence shows, is used by similar types of surveillance legislation (I.e. Germany as G10 Act as discussed in the ECHR case, Weber[231]) in other European countries. The question is – does it matter that specifics are not mentioned in Acts concerning internet surveillance or should they be considered as materially relevant to considerations of necessity and proportionality? This suggestion coincides with another of my discourse on how alternate methods of internet surveillance (as well as forms of old and new surveillance) could be considered as affecting different degrees of privacy infringement, some methods being theoretically more intrusive.

[231] See. Weber and Saravia v. Germany, [2008] 46 EHRR SE5

For example, one could argue equipment interference as being theoretically more intrusive, given that it requires the forced requisition or physical property. Moreover, both interception and interference can harvest a multitude of types of data. A communication (as it is referred to in the Act) is not confined to text as in an email but also video and audio.

Indeed, one may feel that video data is a greater infringement to their privacy than text, giving credence to the idea that the 'types of data' one is likely to intercept should factor into the test of necessity and proportionality. Of course, whether certain types of surveillance offend sensibilities more than others is simply a matter of opinion and can vary greatly from person to person. That is not to say that subjective stances don't work their way into law when they are shared sufficiently (consider the European Consensus doctrine, for example). Subjective opinions becoming part of the legal reasoning is something that I think is exemplified in the case, Malone.[232]

This brief commentary on some aspects of the IPA 2016 will form part of my consideration of the Act in view of ECHR jurisprudence. I hope to expand on these issues more with the aim of drawing some tentative conclusions on whether they bare any significance on whether the Act adequately fulfills its human rights obligations under Article 8 ECHR. This is what I will move onto next.

2.7 Conclusion to Chapter 2

With this Chapter, I have aimed to provide a clear and precise summary of the salient provisions of the Act so as to provide a solid foundation for further analysis.

I am keen to emphasize the fact that the IPA 2016 is not entirely original. Indeed much of its contents (primarily those on interception and equipment interference) have existed prior to the passing of the IPA, in the form of RIPA and other Acts, for nearly two decades which formed part of a broader surveillance remit that also included covert human intelligence sources. As such, much of what I will go on to say about the IPA can, in many places be applied to RIPA as well. Notwithstanding, the IPA is quite groundbreaking in its inclusion of clauses on data retention notices and authorizations. It signifies a key evolutionary stage of UK surveillance law, attempting a more comprehensive incorporation of the Internet,

[232] See. Malone v. the United Kingdom, [1984] 7 EHRR 14

law-makers recognizing how it has become such an intimate part of our lives and how browsing habits can provide an invaluable window into our souls. For me, these provisions are of the greatest concern, especially given the apparent lack of safeguards. I am keen to analyze the ECHR jurisprudence to see the judgment provide any clues as to the legality of such measures.

The last part of the chapter was just to underline aspects of the IPA 2016 which I deem to be germane to considerations of privacy and the right to privacy. They also serve as a springboard from which to analyze the ECHR jurisprudence; do they consider these issues in a meaningful extent, such as ideas of 'intrusiveness'? If not, extrapolating from past dictums, are there any indications as to what conclusions they would draw?

I will continue with a brief explanation of Article 8 ECHR and the tests that have emerged hitherto, with which surveillance methods have been qualitatively assessed regarding their compliance with Article 8.

3 The IPA 2016 vs. Article 8, ECHR

Before engaging with the question of my thesis, I will attempt to briefly summarize the key elements of Article 8 ECHR as well as the methodologies applied by the ECtHR when considering whether a particular practice or law is in breach. I feel that this will serve as a useful starting point.

3.1 Article 8§1 ECHR

Article 8§1 states that:

> Everyone had the right to respect for his private life, his home, and his correspondence.

As one can see, there is no explicit mention of surveillance with the key terms this Article being: 1) private life 2) family life 3) home and 4) correspondence. The first question is; how has the ECtHR interpreted these terms and can forms of Internet surveillance be considered as falling within their ambit?

3.1 (a) ECtHR Article 8 Jurisprudence: broadening the concept of private life

As identified by Boehm [233], the ECtHR has established one overarching principle concerning Article 8§1. This is namely that: private life is a 'broad term not susceptible to exhaustive definition.'[234] The principle coincides with the ECtHR's seeming unwillingness to state, in a precise or consistent way, what types of content can be considered as falling within Article 8§1.[235] Indeed, some have seen fit to label the court's conceptions of private life as 'ill-defined and an amorphous.' [236] Notwithstanding, one could see the origin of this approach as deriving from the ECtHR's treatment of the ECHR as a 'living instrument' that 'must

[233] Boehm, F.(2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, Springer-Verlag Berlin Heidelberg, pp.28
[234] See. Peck v. United Kingdom, [2003] 36 EHRR 41, §57; Niemietz v. Germany, [1992] 16 EHRR 97, §29; Pretty v. United Kingdom, [2002] 35 EHRR 1, §61
[235] Moreham NA, 'The right to respect for private life in the European convention on human rights: a re-examination', European Human Rights Law Review (1): 44-42, pp. 44, 45
[236] ibid. pp.44 - 45

be interpreted in the light of present-day conditions.'[237] By refusing to specify what private life is, the ECtHR prevents inadvertently stymying itself in producing new interpretations in response to technological developing or cultural changes.

It is fairly clear from the case law that the ECtHR does regard the idea of personal data protection and surveillance (as a part and parcel of the idea of personal data protection) as falling within the ambit of Article 8§1 while managing to keep it 'logically…within the boundaries.'[238] So, how have the ECtHR achieved this?

Klass and Others[239] was one of the earliest cases to be brought before the ECtHR under Article 8 and directly addresses, what can be considered as, forms of surveillance. It concerns a piece legislation enacted by the German government entitled; Restrictions on the Secrecy of Mail, Post and Telecommunications Act, which, in certain circumstances, permits the 'competent authorities…' to 'open and inspect mail and post, read telegraphic messages, listen to and record telephone conversations.' [240] Given that Article 8§1 expressly concerns '…home and correspondence…' the relevance of the aforementioned legislation's content is fairly uncontentious. There was brief discourse as to whether 'telephone conversations' constituted 'correspondence', to which the court answered in the affirmative (in line with the opinion of the European Commission). [241]

Thus far, from the perspective of surveillance and data protection, the literal scope of Article 8§1 seems fairly restrictive. Niemietz[242], however, was a landmark case that intentionally broadened the concept of private life. It came at a time when previous judgments seemed intent on developing and crystallizing Article 8§1's exact content.[243] According to Boehm, it was this case that allowed for future expansion of Article 8§1 'in light of the current data protection context' and surveillance concerns.[244]

One way the judgment arguably achieved this was to separate the notion of private life from that of the home or the private sphere. The court states

[237] See. Tyrer v. The United Kingdom, [1978] 2 EHRR 1, §31 and Loizidou v. Turkey, [1995] 20 EHRR 99
[238] Op.cit. Boehm, pp.28
[239] Klass and Others v. Germany, [1978] 2 EHRR 214, §10
[240] ibid. §17
[241] ibid. §41
[242] Op.cit Niemietz
[243] Op.cit. Boehm, pp.29
[244] Op.cit. Niemietz, §29

that one's 'inner circle[245]' is, indeed, an important part of the notion of private life but does not serve to limit its application. The court continues by saying that Article 8 should also encompass 'the right to establish and develop relationships with other human beings'. This is used as a justification for private life not excluding activities outside the home (including those of a 'professional or business nature') given that these present the greatest opportunities in which one can 'establish and develop' relationships.

Admittedly, the argumentation in Niemietz does strike me as being rather unclear and it is difficult to distinguish the main thrust of the argument. That said, for me, the judgments main importance is the way in which it chooses to focus on this idea of relationships, a concept so vague so as to potentially expand Article 8 to all things considered 'part and parcel[246]' of life. This is, in my view, essentially how Niemietz establishes the path for wider consideration of data protection and surveillance issues under Article 8.

3.1(b) ECtHR Article 8 Jurisprudence: The right to data protection/The right not to be put under surveillance

The principles inherent to the Niemietz judgment have subsequently been reiterated and expanded in a number of cases.[247] This has served to cement the persuasive authority of this decidedly vague and all-encompassing interpretation of Article 8 and has led to the creation of the subordinate right to data protection, which is also exceedingly broad in its scope.

Indeed, as elucidated by Boehm[248], when discussing the scope of the right to data protection the court refers to Council of Europe Convention No.108 on data protection whose function is to '…secure…for every individual …respect for his rights and fundamental freedoms, an in particular for his right to privacy with regard to automatic processing of personal data relating to him'[249] while data is described as 'any information relating to an identified or identifiable individual.'[250] The two

[245] Op.cit. Niemietz, §29; a place in 'which the individual may live his own personal life as he chooses and to exclude therefore entirely the outside world not encompassed within that circle.'
[246] ibid.
[247] P.G. and J.H. v. United Kingdom, [2008] 46 EHRR 51, §56
[248] Op.cit. Boehm, pp.41
[249] Council Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending [2006] L105/54, Article 1
[250] ibid. Article 2

defining features of the right to data protection thus seems to be 1) there is information and 2) the information must be of a personal nature.[251]

Some of the cases brought under Article 8 in relation to personal information (contained in the HUDOC's 'person data protection' factsheet[252]) have concerned the improper storage, use, retrieval or destruction of 1) health and medical data (Chave nèe Jullien[253], L.L[254] and L.H.[255]) 2) DNA and fingerprints (S. and Marper[256]) 3) Police files/caution data (B.B[257] and Dimitrov-Kazakov[258]) and 4) other personal data (Peck[259]). For a case to qualify under Article 8, it is not necessary for the data to have been stored, used, retrieved or destroyed in any particular way[260]. As stated, it is only necessary for the application to be about types of 1) information and 2) that the information is of a personal nature. Notwithstanding, the large majority have factual circumstances that detail acts of police surveillance. In this sense, the established right to data protection can similarly be seen as a right not to be put under surveillance (something to which HUDOC makes reference through its mass surveillance document).[261] Naturally, Internet surveillance would be included within this.

3.2 Article 8§2 ECHR

Article 8§2 ECHR states as follows:

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

---

[251] Op.cit. Boehm, pp.12
[252]ECHR Press Unit, 'Personal data protection', , (http://www.echr.coe.int/Documents/FS_Data_ENG.pdf)
[253] See. Chave nèe Jullien v. France, Application No. 14461/88
[254] See. L.L. v. France, ECHR 2006-XI
[255] See. L.H. v. Latvia, [2014] ECHR 515
[256] See. S. and Marper v. the United Kingdom, [2008] ECHR 1581
[257] See. B.B. v. France, ECHR 1998-VI2595
[258] See. Dimitrov-Kazakov v. Bulgaria, Application No. 11379/03
[259] Op.cit. Peck v. United Kingdom
[260] Op.cit. Boehm, pp.12
[261]ECHR Press Unit, 'Mass surveillance', , (http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf)

3.2(a) In accordance with the law

This essentially stipulates that any interference with Article 8 must be prescribed in domestic law. It is not sufficient for an interference to be merely included in the law, however. The law in question must also meet a number of standards, so as to ensure that it is of sufficient quality. These standards have been established and developed by a number of ECtHR judgments and can be accurately described as the following: 1) compliance with the rule of law 2) accessibility and 3) foreseeability.

Underlining these three criteria is the idea that any interference by the public authorities should not be arbitrary[262] and that safeguards should be included in the law to guard against it. In terms of ECtHR jurisprudence, the concept of foreseeability has been their main focus.

The Sunday Times Case[263] deems the law must be foreseeable on the basis that: 'You cannot enjoy or exercise the right to freedom of expression if the enjoyment of such right is made conditional and subject to a law or a rule or principle abounding in uncertainties'. The judgment goes on to state that; laws should be 'formulated with sufficient precision to enable citizens to regulate his conduct…' so he can 'reasonably foresee the consequences which a given action could entail.'[264]

In cases of secret surveillance, this does not necessarily mean that the subject in question should be informed of the fact that they are being subjected to such measures (and thus undermining its value).[265] It has simply been taken to mean that, where such practices are permitted, there must exist comprehensive and clear and rules as to when it can be employed.

3.2 (b) Necessary in a democratic society

As covered by Article 8§2 ECHR, the state can lawfully interfere with the 'right to privacy' if the interference is considered 'necessary in a democratic society' in interests of national security, public safety, economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. The ECtHR is perpetually honing and developing these definitions.

[262] Op.cit. Malone, §88
[263] See. The Sunday Times v. the United Kingdom, [1992] 14 EHRR 229
[264] ibid. §49
[265] Op.cit. Weber

The cases Silver[266], Kvasnica, and Kennedy[267] interpret 'necessary in a democratic society' as requiring a determination on a) whether the interference in question is responding to a pressing and legitimate social need and b) whether the interference is 'proportional' in its response to the social need[268] (otherwise known as the test of proportionality). Whether something is proportional depends on the "seriousness of the interests at stake and the gravity of the interference." This is, naturally, is entirely dependent on the precise factual circumstances of the case. [269][270][271] The state is generally afforded a wide margin of appreciation on these matters but this is adjusted to account for questions of proportionality. When a response is considered disproportionate, the margin of appreciation is interpreted more narrowly.

Something that is commonly utilized in the application of the doctrine of proportionality is The European Consensus Standard. The standard is not applied in a uniform manner given the differing views on what consensus implies.[272] Notwithstanding, it is generally held to refer to the court's consideration of how the other Member States deal with matters of a similar nature; how do they respond to this social need? This is used to determine whether or not the margin of appreciation is wider or narrower in a given case. If a state is found to achieve the same ends using a less intrusive method, then the margin of appreciation will be made narrower unless the circumstances can be sufficiently distinguished.[273]

3.2(c) Conclusion to 3.2

Here I have provided a brief introduction to some concepts that will help me determine whether certain laws and practices in the UK are in breach of Article 8. These concepts can be essentially refined into two key ideas; 1) foreseeability and 2) necessity. As I have discussed, both of these respond to the relative intrusiveness of the interference. With foreseeability, the more intrusive the measure, the more precise and detailed the domestic law must be. With necessity,

[266] See. Silver v. the United Kingdom, [19890] 3 EHRR 475
[267] See. Kennedy v. the United Kingdom, [2010] ECHR 682, §154
[268] Op.cit Silver
[269] Op.cit. Boehm, pp.58
[270] See. Z. v. Finland, [1997] 25 EHRR 371, §75

[272] L.R Helfer, 'Consensus, Coherence and the European Convention on Human Rights', 26 Cornell International law Journal (1993), pp. 133, 135
[273]See. Rasmussen v. Denmark, [1984] ECHR 17

the more intrusive the measure, the narrower the margin of appreciation and the less likely that it will be considered as proportional to achieve the aim pursued.

3.3 Analysis of the legality of the IPA 2016 under Article 8

In my overview of the IPA 2016 in Chapter 2, I divided the act into four parts, these being: 1) interception of communications (targeted and bulk) 2) equipment interference (targeted and bulk) 3) Obtaining communications data and 3) Notices following 'authorization' and data retention. This chapter will consider these collectively, albeit providing due concern for the differences between them.

My analysis will begin with whether the element in question is foreseeable and then I will move on to the question of necessity. In order to hone my research, I will be primarily considering those ECHR cases, which have dealt with the legality of domestic legislation and its practical applications under Article 8. Indeed, as noted by the Court in the Weber[274] application: 'the mere existence of legislation which allowed a system for the secret monitoring of communications entails a threat of surveillance for all those whom the legislation must be applied.' There will be a particular emphasis on laws concerning methods of Internet surveillance although, given the distinct lack of complete decisions in this area (the majority of them pending with the Court merely 'noting' the applications), I will consider cases that involve other forms of new surveillance (such as the interception of telephone calls). Through these, I will attempt to extrapolate the court's response to comparable forms of Internet surveillance, in terms of levels of 'intrusiveness' as well as their response to the IPA 2016. I will also limit my research to those, which involve state surveillance as opposed to the use of surveillance by private organizations or actors.

3.3 (a) In accordance with the law; foreseeability

Many of the cases concerning surveillance commence with a consideration of the measures' compatibility with Article 8(2)'s 'in accordance with the law requirement'. As discussed, this necessitates an assessment of the foreseeability of the law in question. As highlighted in Chapter 3.2, foreseeability does not express the requirement that "an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his

[274] Op.cit. Weber

conduct accordingly."[275] This only serves to belie the 'secret' and 'special context' in which it is instigation. Indeed, this interpretation of foreseeability has gone onto form somewhat of a legal precedent, being repeated in the surveillance cases: Malone, Leander, and Rotaru amongst others. Instead, foreseeability is interpreted as referring to whether the measures under dispute are sufficiently clear so as to "give an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to any such measures."[276] This is viewed as being particularly necessary due to the fact that "the technology available for use is continually becoming more sophisticated."[277]

On a brief side-note, what is particularly interesting is the way that the latter statement seems to suggest that the law must evolve alongside technology i.e. where technology has developed an added dimension of sophistication, resulting in a greater potential for abuse; the legal safeguards dictating its use should be more demanding. The technology considered in Zakharov is referred to as interception, the same term used by the IPA 2016. Whether the relative sophistication of surveillance technology affects the court's assessment of whether the law strikes the right balance is something that I will consider in Chapter 3.4.

Notwithstanding, pieces of legislation that fail to achieve adequate levels of clarity concerning the parameter within which certain surveillance methods can be used, increases the risk of them being used in an arbitrary fashion. The concept of 'arbitrariness' is one of the fundamental limbs of Article 8(2) ECHR's 'test of necessity'. This is where a lot of cases start with an assessment of foreseeability. As you can see, the tests of foreseeability and necessity are very closely intertwined in this respect. This is exemplified by Zakharov given the fact that there are no clear indicators as to when the judgment's considerations of foreseeability end and their application of the test of necessity begins. This was also explicitly mentioned in the Dragojevic, §89 whereby the court opts to consider both 'in accordance with the law' and the 'necessity' test due to them being 'closely related.'

I will progress onto the court's dialogues on whether surveillance legislation achieves the requisite level of clarity and precision in the scope of application of their provisions in the next section.

[275] See. Roman Zakharov v. Russia, [2015] ECHR 1065, §229
[276] ibid.
[277] ibid.

3.3 (b) Necessity and Proportionality

Klass constitutes one of the earliest surveillance cases brought before the ECHR and, as such, goes through all the motions when considering whether methods of secret surveillance are in breach of Article 8(2). Indeed, in the early stages of the judgment, the court feels it necessary to mention that 'the development of terrorism in recent years…' and 'highly sophisticated forms of espionage' means that it is necessary for states to undertake 'secret surveillance subversive elements' in order to 'counter such threats.'[278] This merely has the effect of not completely ruling out the legality of the use of secret surveillance in line with Article 8(2). Although the statement is broad, failing to refer to any specific methods of surveillance. Notwithstanding, it is from this point that the tests of 'necessity and proportionality' have been developed.

The first issue that courts tend to address in their application of the test of 'necessity and proportionality' is whether the law or measures in question had a 'legitimate aim' (See. chapter 3.2 (a)).

This was an uncontentious issue in Klass[279], with the aims of the relevant act being drafted clearly and precisely. Indeed, the aims of the 'Restrictions on the Secrecy of Mail, Post and Telecommunications' Act (otherwise known as 'G10') are stated as being: to protect against 'imminent dangers' threatening 'the free democratic and constitutional order'[280]. The Court considered this as being within the ambit of the 'legitimate aims' provided for by Article 8 (2), namely: 'to safeguard national security and/or to prevent disorder or crime.'[281]

In all the cases following Klass (such as Weber, Kennedy, and Szabo), the issue of 'legitimate aim' has received the minimum degree of attention. This is namely due to the fact that the domestic law permitting activities such as secret surveillance, at the very least, allude to the fact that it is in the name of protecting 'the interests of national security, public safety, the economic well-being of a country…'[282] within its provisions. Moreover, the fact of the legislation in question pursuing a 'legitimate aim' is not often subject to contestation by the applicants. If we direct our attention to the provisions of the IPA 2016, the fact that the Act is pursuing one of Article 8(2)'s legitimate aims is not only stated time and time again by a whole host of related documents, it is also a key component upon

[278] ibid. §48
[279] Op.cit Klass
[280] ibid. §45
[281] ibid. §46
[282] Op.cit Weber, §107

which an equipment interference or interception warrant or authorization can be issued (see. Part 2 Chapter 1, §18, §19 and §20 IPA 2016).

After 'legitimate aim' is considered (often in brief), the court then moves on to the questions of 'necessity and proportionality'. Klass provides an early outline of the court's methodology in respect to the application of 'necessity and proportionality' test. It that; 'whatever system of surveillance adopted' the court must be satisfied that there exists 'adequate and effective guarantees against abuse.' It clarifies that this test is 'relative in character', depending on the 'circumstances of the case' such as the nature, scope, and duration of possible measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law.'[283] It was noted in Weber that the 'national authorities enjoy a fairly wide margin of appreciation in choosing the mean for achieving the legitimate aim.'[284]

Klass & Weber

The applicant's main complaint in Klass, stemmed from the fact that the G10 did not provide for the notification of individuals who had been subject to secret surveillance or to the extent that their 'rights were interfered with'[285], prohibiting them from seeking legal in the domestic courts. The applicant's believed that this was of paramount importance to ensure that the government did not use their powers of surveillance in a manner that was disproportionately excessive. Of course, the IPA 2016 resembles the G10 in this sense, that such provisions concerning interception of communications and interference of equipment, does not provide any post-facto notification system for those who have been subjected to such measures. In Klass, the court found that, not providing such notifications for recently suspended surveillance measures (or providing such notifications only in very limited circumstances[286]) was necessary in order to achieve the Act's legitimate aim given that providing such notifications could 'jeopardize the longer-term purpose that originally prompted the surveillance'[287] and possibly 'reveal the working methods of the investigation' and lead to the identification 'of their agents'.[288] For the provisions of the Act to negatively effect the efficacy of the interference it permits

[283] ibid. §50
[284] Op.cit Weber, §106
[285] ibid, §58
[286] ibid. §11 and 19
[287] ibid. §58
[288] ibid.

would go to essentially contradict the principle of necessity. It was on these grounds that the court ruled against the applicants. From this, one can hasten to make the conclusion that the ECtHR would treat the IPA 2016 in a similar regard.

In Klass, the court emphasized that the legal safeguards and oversights provided for in the Act made it so that the relevant provisions would 'reduce the effect of the surveillance measures to an absolute minimum'[289], thus rendering the Act proportional. These conditions are found at § 51 - 54 of the judgment and I will go on to consider them in further detail in due course.

Weber also concerned the G10 (albeit the amended version), specifically section 3 ((1) – (5)) that legislated for 'strategic monitoring of telephone communications', which the applicant believed provided for monitoring powers that were 'far too wide'[290] and did not 'correspond to a pressing need on the part of society for such surveillance.'[291] Like in Klass, the German government responded by insisting that such provisions were 'necessary to combat international terrorism'[292] with Europe facing an increasing threat from 'Al-Qaida following the terrorist attack of 11 September 2001.' [293] The government also mentioned that it was important to prevent international arms trafficking and it was impossible to 'counter these threats' without access to the 'strategic monitoring of telecommunications.'[294]

The court also found in the government's favor, deeming that they had struck a reasonable, proportional balance through their 'limitation of the offenses through which data transmission was permitted' [295] and by 'the provision of supervisory mechanisms against abuse.'[296] Regarding the G10's inclusion of various supervisory mechanisms, the court highlighted that they essentially remained the same as those contained in the previous version considered in Klass (See. Above) and saw no reason to alter their decision in this regard. Indeed, the G10 makes it so that surveillance can only be ordered by a written application by the head of the security services with a 'Federal Minister empowered for the purpose'[297] giving the final say. There are also conditions concerning the implementation of surveillance

[289] ibid. §59
[290] Op.cit Weber, §111
[291] ibid. §112
[292] ibid. §109
[293] ibid.
[294] ibid.
[295] ibid. §129
[296] ibid.
[297] ibid. §51

measures, the time in which the surveillance measure can 'remain in force', what happens to data that has been obtained during the course of the surveillance amongst others.

Regarding the Act's 'limitation of offenses through which data transmission was permitted', the Court noted that the amendments made had 'considerably extended the range of subjects in respect of which' strategic monitoring 'could be carried out under section 3(1).[298] This was the source of the applicant's central point of contention, he deeming that some of the subjects included on the list were not 'such a pressing need on the part of society'[299] that it justified the use of such intrusive measures. Moreover, increasing technological capabilities meant that it now possible to 'identify the telephone connections involved in intercepted communications.'[300] In the applicant's view, these factors combined to make the amended G10 disproportional.

Whereas the original G10 (as considered in Klass) only permitted such monitoring in cases wherein 'order to detect and avert an armed attack on Germany', the amended version contains a list which also permits monitoring in cases that fall within an exhaustive list of broadly defined 'serious offences'[301] found in section 3(1) (one of these being 'counterfeiting money abroad'). In consideration of this, the ECtHR still maintained the amended legislation as being proportional. The court referred back to the restrictive safeguards, oversights, and limitations on powers included in the original G10 as being still adequate to satisfy the test of proportionality, even in view of the amended section 3(1). Moreover, it highlighted the fact that the additional 'serious offenses' listed still had notions of 'national security, public safety or the economic well-being of the country' at their core[302], but this was only a minor additional point.

The provisions of the IPA 2016 that bear the closest resemblance to those disputed in this are those concerning the interception of communications. Given their close resemblance, it is reasonable to suggest that the court would have also found this portion of the IPA 2016 to be in keeping with Article 8 in this regard.

[298] ibid. §114
[299] ibid. §112
[300] ibid. §115
[301] ibid. §114
[302] ibid. §115

Kennedy

Kennedy v. UK concerns the IPA 2016's legal forebear, RIPA and looks at provisions concerning 'interception of communications.' The court's consideration of necessity begins with an examination of RIPA's provisions that serve limit the government's use of interception techniques. Early in the judgment, the court highlights the link between the test of foreseeability and that of necessity. Clearly defining the acts or categories of people that are liable to have their communications intercepted is intrinsic to preventing the disproportionate use of such techniques, hence its relevance. Following from their considerations of RIPAs foreseeability, the courts were satisfied, believing the categories to be sufficiently clear so as to guard against the 'indiscriminate capturing of vast amounts of communications'[303] which, of course, would be considered as in breach of the test of necessity.

As detailed in Chapter 2 of this thesis, the RIPA and the IPA 2016 employs a warrant system. The court goes on to consider what should be contained in a warrant, specifying that it must 'clearly specify either by name or by description, one person as the interception subject or a single set of premises as the premises in respect the warrant is ordered.'[304] A schedule to the warrant must also contain 'names, addresses, telephone number and other relevant information…'[305] Again, this is imperative for the prevention of using such powers in an indiscriminate way.

'Interception warrants' under the IPA 2016 and RIPA last for 6 months unless canceled earlier.[306] However, the Acts contain provisions on warrant renewal, which makes no stipulations as to the total number of renewals permitted; essentially making the total time a warrant can be in effect indefinite. The court is quick to establish that RIPA's decision to omit such provisions is not disproportionate to the Act's aims, given the fact that the complexity of cases may mean that investigation will take an inordinate length of time to complete.[307] This is, of course; only as long as there are adequate safeguards exist so as to limit the potential for abuse. Given that a renewal is subject to the same safeguards as creation and existing warrants must also be canceled if they fall short of these safeguards[308]

[303] Op.cit. Kennedy v. UK, §160
[304] ibid.
[305] ibid.
[306] Op.cit. Explanatory notes, pp. 23, §107
[307] Op.cit. Kennedy, §161
[308]Op.cit. RIPA, Section 9(3)

(requiring them to be under a constant state of review), the court was satisfied in this regard.

The ECtHR goes on to examine RIPA's procedures for the examination, use, storage, processing, communication and destruction of intercepted material, detailing to relevant provisions.[309] In detailing their salient elements, the Court was satisfied that they 'provided adequate safeguards for the protection of data obtained.'[310]

RIPA's supervisory provisions are also considered with the court noting that that, given the fact that abuse is 'potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole' it is 'desirable to entrust supervisory role to a judge.' That said, the judgment communicates satisfaction that the Investigatory Powers Tribunal (IPT), established by the act, is suitably impartial, informed and independent to carry out this function. Satisfaction is also expressed towards the IPT's mandated powers, enabling them to authorize, execute and cancel warrants as well as their role as arbitrators of complaints levied by members of the public.[311] Moreover, the publication of the IPT's 'legal rulings', add to RIPA's relative transparency. All in all, the ECtHR, in this case, found that there was no breach of Article 8.

In line with the ECtHR's approval of RIPA, what would their opinion be of its legal descendant, the IPA 2016? Well, as discussed, the IPA 2016 is more of a consolidation of past surveillance laws, drawing heavily from RIPA. While IPA 2016 does make numerous changes and additions to UK surveillance law making the scope of its application potentially broader in terms of interception of communications, it doesn't deviate from RIPA to any great extent. In this sense, I believe that the ECtHR would find in favor of the provisions concerning the categories of person or situation in which a targeted inception warrant can be issued under the Act, possibly regarding them as being sufficiently precise (that is not to say that the ECtHR would necessarily find the same in reference to anything other than targeted interception).

Regarding the Court's positive stance of RIPA's creation of the IPT as a means of providing judicial oversight for interception warrants, I believe they would also find in favor of the IPA 2016 establishment of the JC and IPC which are, more or less, identical in their remit and composition.

---

[309] Op.cit. Kennedy, §162, §163, §164
[310] ibid. §163
[311] ibid. §167

Szabo and Vissy

This case concerns 'telephone tapping' as contained in Hungary's Police Act and National Security Act.[312] Following previously established ECtHR jurisprudence, the court commences their analysis of Szabo by reiterating what it considers to be the minimum safeguards of law permitting the use of 'telephone tapping'. These were stated to include:

…The definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating data to other parties; and the circumstances in which recordings may or must be erased or destroyed.[313]

In iterating these, the court emphasized that 'to have clear, detailed rules on interception of telephone conversations' is essential 'especially as the technology available for use is continually becoming more sophisticated.'[314] Of course, whether the increasing sophistication of technology materially affects the court's considerations of legislation, seeking to use such technological development for surveillance purposes remains to be seen. I hope to approach the subject in the next chapter.

The applicant's main contention was that the provisions in question were not 'sufficiently detailed or precise to meet the foreseeability requirement.'[315] Whereas foreseeability is typically considered one of the criterions through which the court assesses whether provisions are of sufficient quality to be 'in accordance with the law', in this instance it is integrated with the court's application of the test of necessity. Indeed, as expounded in previous cases, the provisions must be 'sufficiently precise'[316] to guard against abuse and arbitrariness and with due regard to its legitimate aim.

As with previous cases, the judgment concedes to the fact that provisions providing for surveillance powers need not be overly rigid due to the complicated, fast-developing nature of the situations they seek to legislate for.[317]

---

[312] ibid. §60
[313] See. Szabo and Vissy v. Hungary, [2016] ECHR 579, §56
[314] ibid. §62
[315] ibid. §61
[316] ibid.
[317] ibid. §64

The court notes that surveillance legislation must clearly define the types of persons as well as the situations that may give to the interception of communications.[318] It is along these lines that the court takes issue with Section 7/E (3) of the Act in question. This is namely to do with the way the provision seems to equate the notion of "persons concerned identified…as a range of persons'[319] and its potential to allow for the 'unlimited surveillance of a large number of people.'[320] The provision did not impose the requirement that the authorities should first 'demonstrate the actual or presumed relation between the persons concerned…and the prevention of any terrorist threat.'[321] Only then, can the test of necessity be adequately applied.

In reference to my consideration of the 'thematic' nature of the IPA 2016's equipment interference warrants, one can make a connection with the court's findings in relation to Section 7/E (3). As detailed, there is no requirement in the IPA 2016 to show that a person has a material connection with the threat prompting the investigation; it must only be showed that there is a link between that person and the individual who may be the key focus of the investigation. This link could have been in the past as well as the present (the same goes for organization or locations that may be subject to an equipment interference warrant). From this, we can assume that the court would not be in favor of this particular provision and, may deem it to be contrary to Article 8 (2).

That said, Section 7/E considers in Szabo and Section 101, IPA 2016 deal with the acquisition of communications data and secondary data via different means: through interception in the former and equipment interference in the latter. One might speculate that 'thematic warrants' are somehow more practical and appropriate for equipment interference, unlike interception. This could be related to the fact that particular pieces of equipment can have their locations frequently changed, be used by many different people and organizations, necessitating a broader and more undefined approach to warrant criteria. Such considerations may change the Court's mind in this regard. It is, however, impossible to really say one way or the other with reference to the established jurisprudence.

[318] ibid. §66
[319] ibid. §67
[320] ibid.
[321] ibid.

Kruslin

This telephone-tapping case resembles *Szabo* - the court taking issue with how the piece of French surveillance law in question 'does not indicate with reasonable clarity the scope and manner of the exercise of the relevant discretion confers on the public authorities.'[322] Indeed, in this case, the law was found in breach of Article 8. Admittedly, this is a comparatively more clear-cut case given the fact that no specifications were made concerning 'the categories of people liable to have their phones tapped by judicial order and the nature of the offenses that might give rise to such an order…'[323], thus it was not necessary to go into the technicalities.

3.4 Commentary on Chapter 3.3; the issue of comparative intrusiveness

The issue of comparative intrusiveness is communicated numerous times by ECHR case-law concerning internet surveillance. Indeed, in Szabo, the court emphasizes that, in response to the development of 'cutting-edge technologies' that are able to massively monitor communications and automate the systemic collection of data, legal safeguards securing respect for citizen's Convention rights must be developed 'simultaneously'.[324] It was on this basis Szabo was distinguished from Kennedy. Whereas the 'impugned legislation' in the Kennedy case did not "allow for the 'indiscriminate capturing of vast amounts of communications,'" in Szabo, this was the perceived effect of the 'broad-based provisions' of the legislation under consideration (The National Security Act).[325] This was viewed as the key reason by which Kennedy was deemed not to be in breach of Article 8. Notwithstanding, the court also made reference to the types of information that are vulnerable to collection in their considerations, stating them as representing the 'most intimate aspects of citizens' lives.'[326]

[322] See. Kruslin v. France, Application no. 11801/85, §36
[323] Ibid. §35
[324] Op.cit Szabo,§68
[325] Ibid. §69
[326] Ibid. §70

4 Conclusions and final remarks

Now I will attempt to draw some tentative conclusion and final remarks on all that I have considered throughout this thesis.

In terms of the compatibility of the IPA 2016 with Article 8 ECHR, I believe that certain parts are in line with the case-law I considered, and other parts are not. Notwithstanding, the parts of the IPA 2016 that I find the most concerning (the provisions on retention notices and authorizations) have not yet seen any specific consideration by the ECtHR with case law being confined to telephone tapping, bulk and targeted interception and one instance of metering (Malone). Perhaps it will be the subject of a future case!

The large majority of the Act, I would consider being in compliance with ECtHR jurisprudence given that RIPA was considered in Kennedy v. UK as operating within the law - the two Acts sharing the bulk their interception provisions. There is some doubt about whether the provisions on equipment interference would be permissible given the 'thematic' nature of the scope of their application. Moreover, I think that authorizations would struggle to comply given their seemingly complete lack of the judicial oversight which has been provided for in all other sections.

As you may recall, a large portion of the thesis was committed to discussing how alternative methods of surveillance can be considered more or less intrusive based on the means employed as well as the results achieved in terms of personal data collection. I was also keen to express how the ever-increasing technological sophistication of the modern era and the genesis of the internet meant that internet surveillance can, in theory, be considered as far beyond any other means of surveillance in terms of intrusiveness from both a means and an ends standpoint. One of the things I was searching for in my consideration of ECHR case-law was an indication that the court was paying due to regard to the nuanced privacy implications of alternate surveillance technologies (within the disputed domestic law). I was hoping that such considerations would bear a material effect on the court's judgment concerning a law's compliance with Article 8.

I was not completely disappointed in this regard. Szabo was one judgment whereby the court made explicit reference to how the legal tests deriving from Article 8 should be applied in such a way as to give due regard to the relative

sophistication and reach of a surveillance measure or technology. The ECtHR went on to clarify that, where measures are particularly threatening to privacy, the scope of their application should be drafted with greater clarity and precision. As one progresses through the judgment, one realizes that this statement is lacking in any real meaning. In determining whether the scope of application is sufficiently precise, no reference is made to the technicalities of the surveillance measure in the judgment. In the end, the court finds itself getting mixed up in something of a tautology i.e. the scope of application is too imprecise because the scope of application is too imprecise! At no point are we provided with an insight on how risks to privacy should have a bearing on precision. Of course, this is not to say that this is due to laziness on the part of the court. It is hard to really make these kind of assessments when there aren't a long line of similar cases through which one can attempt to delineate whether the court has a real doctrinal approach to this matter. I was hoping to also see if such consideration would also have ramifications on the application of the test of 'necessity and proportionality' but there is very little by way of clear dictums to this effect in ECHR jurisprudence.

I conclude that – at this point in time – the ECtHR is ill-equipped to adequately consider the vast and expansive ramifications that methods of internet surveillance power on concepts of privacy. The jurisprudence that has been produced is of limited value given the courts limited exploration into the idea of 'intrusiveness' - that I have consistently attempted to draw upon through the entirety of this thesis - as well as a fairly basic comprehension of developing technologies (*Review* Chapter 1.4 (e) of the thesis). I believe that the Internet truly does provide a 'window into our souls' on a scale that has never been seen before, providing the tools to track and record every movement, every thought, and even every fleeting thought. It also provides the tools to send and replicate such data *ad infinitum*. For the law to truly to adapt and change in line with such technology, what is needed it a robust and deep consideration of all the issues. I feel the ECtHR, so far, fails in this regard and as a result, the law's evolution is being hindered. Indeed, the same standards concerning the doctrine of proportionality – are applied to a wide range of technologies in a way that does not seek to differentiate between them in any material way. Cana telephone tapping really be considered as comparable to acts of interception of internet communications? I believe not.

Bibliography

Books

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, Springer-Verlag Berlin Heidelberg

Castells, M. (1999), *The Information Age, Volumes 1-2: economy, Society and Culture*, Oxford: Wiley-Blackwell

C.E. Howard Vincent (1900), *The Police Code and the General Manual of the Criminal Law for the British Empire*, Kent & Co

Cyrille Fijnaut (1979), *Opdat de macht een toevlucht zij? Een historische studie van het politie-apparaat al seen politieke instelling*, Kluwer Law International

Cyrille Fijnaut & Gary T. Marx (1995), *Police Surveillance in Comparative Perspective*, Kluwer Law International

David Wright (2014), *Surveillance in Europe*, Routledge

D.G. Browne (1956),*The Rise of Scotland Yard; A History of the Metropolitan Police*, George G. Harap

Dornberger, Walter (1954), *V-2*, Ballantine

Fuchs, C. (2012), *Internet and Surveillance; The Challenges of Web 2.0 and Social Media*, Routledge

Fuchs, C. & Boersma, K. (2012), *Internet and Surveillance, The Challenges of Web 2.0 and Social Media*, Routledge Studies in Science, Technology and Society

Gray (2013), *Leon, How does GPS Work*, The Rosen Publishing Group

Inder Sidhu (2015), *The Digital Revolution: How Connected Digital Innovations Are Transforming You Industry, Company and Career*, FT Press

Janice Richardson (2017), *Law and the Philosophy of Privacy*, Routledge

J.J. Tobias (1979), *Crime and Police in England* (1700 – 1900), Gill and MacMillan

Karen M. Hess (2013), *Police Operations: Theory and Practice*, Cengage Learning

Kevin D. Mitnick (2011), *The Art of Deception: Controlling the Human Element of Security*, John Wiley & Sons

Kruegle, Herman (2011), *CCTV Surveillance: video Practices and Technology*, Butterworth-Heinemann

L. Radzinowicz (1948 – 1956), *A History of English Criminal Law and its Administration from 1750*, London

Marx, Gary T. (2002), *What's new about the "new surveillance"? Classifying for change and continuity, Surveillance and Society*,

Paul Knepper (2009), *Urban Crime Prevention, Surveillance, and Restorative Justice: Effects of Social Technologies*, CRC Press

Peter Aksoy & Laura DeNardis (2007), *Informational technology in Theory*, Cengage Learning

Peter Wright (1987), *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*, Stoddart

P. Manuel (1790), *La police de Paris dévoilée*, J.B. Garnery

Richard W. Kroon (2014), *A/V A to Z: An Encyclopaedic Dictionary of Media, Entertainment and Other Audio-visual Terms*, McFarland

Senyonovna, Eugenia (1967), *Journey into the Whirlwind*, New York: Harcourt, Brace & World, Inc.

S.H. Palmer (1988), *Police and Protest in England and Ireland 1780 – 1850*, CUP

Soustelle, Jacques (2002), *The Daily Life of the Aztecas*, Phoenix Press

Starke-Meyerring, Doreen and Laura Gurak (2007), *Internet Encyclopedia of privacy*, Greenwood Publishing Group

Zizi A. Papcharissi (2016), *A Private Sphere: Democracy in a Digital Age*, John Wiley & Sons

Cases (ECHR)

B.B. v. France, ECHR 1998-VI2595

Chave nèe Jullien v. France, Application No. 14461/88

Davis & Ors v. SSHD [2016] EWHC 2092

Dimitrov-Kazakov v. Bulgaria, Application No. 11379/03

Kennedy v. the United Kingdom, [2010] ECHR 682

Klass and Others v. Germany, [1978] 2 EHRR 214

Kruslin v. France, Application no. 11801/85

Kvasnica v. Slovakia, [2009] ECHR 872

L.H. v. Latvia, [2014] ECHR 515

L.L. v. France, ECHR 2006-XI

Loizidou v. Turkey, [1995] 20 EHRR 99

Malone v. the United Kingdom, [1984] 7 EHRR 14

Niemietz v. Germany, [1992] 16 EHRR 97

Peck v. United Kingdom, [2003] 36 EHRR 41

P.G. and J.H. v. United Kingdom, [2008] 46 EHRR 51

Pretty v. United Kingdom, [2002] 35 EHRR 1

Rasmussen v. Denmark, [1984] ECHR 17

Roman Zakharov v. Russia, [2015] ECHR 1065

S. and Marper v. the United Kingdom, [2008] ECHR 1581

Silver v. the United Kingdom, [19890] 3 EHRR 475

(The) Sunday Times v. the United Kingdom, [1992] 14 EHRR 229

Szabo and Vissy v. Hungary, [2016] ECHR 579

Tyrer v. The United Kingdom, [1978] 2 EHRR 1

Weber and Saravia v. Germany, [2008] 46 EHRR SE5

Z. v. Finland, [1997] 25 EHRR 371

Cases (UK)

Peter Semayne v. Richard Gresham (1604), 77 ER 194

Davis & Ors v. SSHD [2016] EWHC 2092

Leah v. Money (1975) 97 Eng. Rep. 1075

John Entick, (Clerk) v. Nathan Carrington and Three Others (1765), EWHC KB J98

Legislation

Domestic

Computer Misuse Act 1990

Data Retention and Investigatory Powers Act 2014

Data Protection Act 1998

Investigatory Powers Act 2016

Regulation of Investigatory Powers Act 2000

International

European Convention on Human Rights

Council Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending [2006] L105/54

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1985] ETS No.108

Journal Articles

Hilbert, Martin & López, Priscila, ‘The World's Technological Capacity to Store, Communicate and Compute Information’, Science (2011). 332 (6025): 60–65.

L.R Helfer, ‘Consensus, Coherence and the European Convention on Human Rights’, 26 Cornell International law Journal (1993)

Marx, Gary T., ‘What’s new about the “new surveillance”? Classifying for change and continuity’ (2002), Surveillance and Society, Volume 1 (1)

Moreham NA, ‘The right to respect for private life in the European convention on human rights: a re-examination’, European Human Rights Law Review (1): 44-42

Websites

Andy O’Donnell, ‘What are Packet Sniffers and How Do They Work? 2018, Lifewire, (https://www.lifewire.com/what-is-a-packet-sniffer-2487312

BBC News, ‘UK, Most Watched Nation by CCTV’, 21 July 2009, (http://news.bbc.co.uk/2/hi/uk/8160757.stm)

Big Brother Watch, Investigatory Powers Act Factsheet; Bulk Personal Datasets, 2016, (https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Bulk-Personal-Datasets.pdf)

Big Brother Watch, ‘The Price of Privacy: How local authorities spent £515m on CCTV in four years’, 2002, (https://www.bigbrotherwatch.org.uk/files/priceofprivacy/Price_of_privacy_2012.pdf)

Bill Stewart, ‘IPTO – Information Processing Techniques Office, The Living Internet’, 2000 (http://www.livinginternet.com/i/ii_ipto.htm)

Camilla Graham Wood, Thematic warrants: ‘Destroying democracy under the cloak of defending it.’ (2016), Solicitors Journal (https://www.solicitorsjournal.com/comment/thematic-warrants-destroying-democracy-under-cloak-defending-it)

‘Commons passes emergency data laws despite criticism’, BBC News, 15 July 2014 (http://www.bbc.co.uk/news/uk-28305309)

David Anderson, ‘A Question of Trust; Report of the Investigatory Powers Review’, Independent Reviewer of Terrorism Legislation, 2015, (https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf)

Dominic Casciani, ‘Spy Pictures of Suffragettes Revealed’, BBC News Online, 3 October 2003 (http://news.bbc.co.uk/1/hi/magazine/3153024.stm)

Federal Trade Commission, ‘Monitoring Software on Your PC: Spyware, Adware, and Other Software, Staff Report: Federal Trade Commission’, 2005, (https://www.ftc.gov/sites/default/files/documents/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-and-other-software-report/050307spywarerpt.pdf)

Griffin, A., ‘Investigatory Powers Act Goes into Force, Putting UK Citizens under Intense New Spying Regime’, The Independent Newspaper, 31 Dec 2016 (http://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-act-bill-snoopers-charter-spying-law-powers-theresa-may-a7503616.html)

Griffin, A. ‘The Government Quietly Launched ‘Assault on Freedom’ While Distracting People, Say Campaigners Behind Legal Challenge’, The Independent, 9 Jan 2017 (http://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-act-liberty-legal-challenge-high-court-opposition-a7518136.html)

Griffin A., ‘U.K. spying laws: government introduced law requiring WhatsApp and iMessage to break their own security’, The Independent, 12 March 2016 (http://www.independent.co.uk/life-style/gadgets-and-tech/news/uk-spying-laws-uk-government-introduces-law-requiring-whatsapp-and-imessage-to-be-broken-a6905106.html)

Home Office, ‘DRAFT Code of Practice; Bulk Acquisition’, Autumn 2016, (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557863/IP_Bill_-_Draft_Bulk_acquisition_code_of_practice.pdf)

Home Office, ‘DRAFT Code; Communications Data’, Autumn 2016, (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557862/IP_Bill_-_Draft_CD_code_of_practice.pdf)

Home Office, ‘DRAFT Code of Practice; Equipment Interference’, December 2017, (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/668940/Draft_code_-_Equipment_Interference.pdf)

Home Office, ‘DRAFT Code of Practice; Intelligence Services’ Retention and Use of Bulk Personal Datasets’, December 2017, (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/668933/Draft_BPD-_Intelligence_Services__Retention_and_Use_of_Bulk_Personal_Datasets.pdf)

Home Office, ‘DRAFT Code of Practice; Interception of Communications’, December 2017, (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/668941/Draft_code_-_Interception_of_Communications.pdf)

Home Office, ‘DRAFT Code of Practice; National Security Notices’, December 2017, (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/668939/Draft_code_-_National_Security_Notices.pdf)

Home Office, ‘Factsheet #1 – Communications Data; Data Retention and Investigatory Powers Bill’ (2014), (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/330510/Factsheet_Data_Retention.pdf)

Home Office, Factsheet: Data Definitions, 2016, (https://www.gov.uk/government/publications/investigatory-powers-bill-fact-sheets)

Home Office, ‘Retention of Communications Data Codes of Practice’, 9 December 2014,
(https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/383401/Draft_Data_Retention_Code_of_Practice_-_for_publication_2014_12_09.pdf)

HM Revenue and Customs, ‘Money laundering supervision: an introduction’, 23 October 2014 (https://www.gov.uk/guidance/money-laundering-regulations-introduction)

‘Investigatory Powers Bill: Context’,
(https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/530551/Context_Factsheet.pdf)

‘Investigatory Powers Bill; Factsheet; Targeted Interception’,
(https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473739/Factsheet-Targeted_Interception.pdf)

‘Investigatory Powers Bill; Factsheet – Targeted Communications data’,
(https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473747/Factsheet-Communications_Data_General.pdf)

James Ball, ‘Leak memos reveal GCHQ efforts to keep mass surveillance secret’, The Guardian, 25 Oct 2013, (https://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden)

Jean Camp, ‘The Internet as a Public Space: Concepts, Issues, and Implications in Public Policy’, 2000, John F. Kennedy School of Government, Harvard University, (https://sites.hks.harvard.edu/mrcbg/research/j.camp_acm.computer_internet.as.public.space.pdf)

Lee Raine, ‘Census: Computer ownership, internet connection varies widely across U.S’, Pew Research Centre, 2014 (http://www.pewresearch.org/fact-tank/2014/09/19/census-computer-ownership-internet-connection-varies-widely-across-u-s/)

Liberty, Liberty’s briefing on Part 6 of the Investigatory Powers Bill for Committee Stage in the House of Commons, April 2016 (https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%27s%20Briefing%20on%20Part%206%20of%20the%20Investigatory%20Powers%20Bill%20for%20Committee%20Stage%20in%20the%20House%20of%20Commons.pdf)

MacAskill, Ewen, ‘Extreme surveillance’ becomes UK law with barely a whimper’, The Guardian, 19 Nov 2016
(https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper)

MI5, Bulk Data, (https://www.mi5.gov.uk/bulk-data)

Press Release No 54/14, ‘The Court of Justice declares the Data Retention Directive to be invalid’, Court of Justice of the European Union, 8 April 2014
(https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf)

Press Unit ECHR, ‘Mass surveillance’, (http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf)

Press Unit ECHR, ‘Personal data protection’, (http://www.echr.coe.int/Documents/FS_Data_ENG.pdf)

‘Regulation of Investigatory Powers Act 2000; Explanatory Notes’, (http://www.legislation.gov.uk/ukpga/2000/23/notes)

Sir Ronnie Flanagan, ‘A Report on the Investigations by Cambridgeshire Constabulary into the Murders of Jessica Chapman and Holy Wells at Soham on 4 August 2002; Summary of Conclusions and Recommendations’ (2002), (https://www.justiceinspectorates.gov.uk/hmicfrs/media/investigation-by-cambridgeshire-constabulary-20040530.pdf)

Unknown, ‘Regulation of Investigatory Powers Act 2000’, The Guardian, Monday 19 January 2009, (https://www.theguardian.com/commentisfree/libertycentral/2009/jan/14/regulation-investigatory-powers-act)

Weaver, M., ‘MI5 resisting independent oversight of bulk data collection’, The Guardian, 26 July 2016 (https://www.theguardian.com/uk-news/2016/jul/26/mi5-resisted-independent-oversight-of-communications-data-collection)

Parliamentary Debates

Baroness Jones of Moulsecombe, ‘Data Retention and the Investigatory Powers Bill’, House of Commons Debate, 15.07.2014

House of Lords & House of Commons Joint Committee on the Draft Communications Data Bill, ‘Draft Communications Data Bill’ (2012 – 13),

Cooper, Yvette, ‘Data Retention and the Investigatory Powers Bill’, House of Commons Debate, 15.07.2014

May, Theresa, ‘Data Retention and the Investigatory Powers Bill’, House of Commons Debate, 15.07.2014

The Lord Bishop of St. Albans, ‘Queen Speech Debate in the Lords Chamber’, 24.05.2016

Baroness Jones of Moulsecombe, ‘Data Retention and the Investigatory Powers Bill, House of Commons Debate’, 15.07.2014