Is UK surveillance law suitable for the digital age?

Clowance Rose Pearl Wheeler-Ozanne

Law School, University of Strathclyde
Doctor of Philosophy
2018

Declaration of Authenticity and Author's Rights

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.

Parts of this thesis (Chapters 1 and 3) were presented as work in progress at the following conferences:

- *Postgraduate Law Conference,* Queen Mary University of London, June 2016
- *SLSA Annual Conference*, Newcastle University, April 2017

Signed:

Date: 5th of September 2018

Acknowledgements

As is custom, I would like to thank those who have assisted, encouraged and supported me throughout this PhD. First, I would like to thank my supervisors, Dr Genevieve Lennon and Ms Therese O'Donnell, for providing me with unwavering support and advice throughout this entire process. To Genevieve especially, not only have you helped to develop my academic abilities, you have helped give me the confidence I lacked at the start of this journey to believe in myself. I would also like to thank Professor Mike Nellis who I look to not only as a mentor, but as a friend. Without Mike, I would never have found my passion in surveillance or, perhaps more importantly, had the courage to pursue it.

To my parents, despite the distance you have been there day and night, as always. I never expected any less, but I still can't thank you enough. Dad, the sky really is the limit. To my husband Scott, as I said on December 30th, thank you for taking on my ambitions and dreams as your own and for being every member of my family when I've needed them the most. I could not have done this without your love, patience, kindness and support. Finally, thank you Tiny Toes - the very best of surprises that has motivated and inspired me to cross the finish line smiling.

Abstract

This thesis examines the suitability of UK surveillance law for the digital age in terms of its protection of privacy. It argues that UK law regulating state surveillance fails to recognise the undulations of the contemporary surveillance landscape brought about by the digitalisation of society and that this has negatively impacted both individual and societal interests in privacy. Privacy is underlined as a cornerstone of liberal democratic society that continues to be relevant and worthy of legal protection in the digital age. It is argued that the legal tradition needs to engage more fully with other disciplines, particularly surveillance studies, to ensure that expectations of privacy within the digital age are properly reflected, and protected, by law. This thesis helps bridge this gap by adopting a multidisciplinary approach to the assessment of UK surveillance law. In particular, it is argued that the ownership of surveillance has been democratised in the digital age, enabling the individual to participate in surveillance. It is argued that, this too, needs to be recognised in order to protect the benefits of the contemporary surveillance landscape bestowed on civil society. The main argument of this thesis is that the law needs to attune to the technological and cultural changes the contemporary surveillance landscape has undergone in order to preserve privacy in the digital age. This thesis concludes with recommendations as to how UK surveillance law can be improved so that this can be achieved.

Introduction

This thesis examines the suitability of the Investigatory Powers Act 2016 ('IP Act') in the digital age in terms of its protection of privacy as defined under Article 8 of the European Convention on Human Rights ('ECHR'). The IP Act is now the major piece of legislation covering most state surveillance powers in the UK, although given that not all powers are contained within this law, reference is made to other statutes where necessary.

The core argument of this thesis is that UK law regulating state surveillance does not adequately protect privacy in the digital age because it fails to properly recognise the technological and cultural changes that the contemporary surveillance landscape has undergone. This thesis will propose three ways in which the law can and must become more attuned to the technocultural realities of the digital age if privacy is to be preserved. These are: (i) re-constructing traditional boundaries (such as, the public-private dichotomy); (ii) recognising the role of the individual as both a source and object of surveillance; and, (iii) enhancing protection for group privacy.

In addition, this thesis argues that legal modifications in the above areas will also protect the benefits that the contemporary surveillance landscape has bestowed on civil society, where digital data exchanges (in which surveillance is always immanent) has become integral to commerce and everyday life, 'part of a way of seeing and of being in the world…of a whole way of life.'[1] Lyon calls this the 'culture of surveillance.'[2]

Whilst the 'culture of surveillance' is increasingly recognised and debated in surveillance studies literature, legal scholars tend not to engage with surveillance beyond a black letter level, failing to take stock of the 'social and cultural processes within which surveillance is embedded.'[3] Cohen describes the law as 'black-boxing'

---

[1] David Lyon, *The culture of surveillance* (Polity Press, 2018) 30. Lyon uses Raymond Williams' definition of 'culture' as a 'whole way of life' here, see Raymond Williams, *Culture & society: 1780-1950* (Chatto & Windus, 1958). See also, David Lyon, *Surveillance after Snowden* (Polity, 2014) 3-4.
[2] Ibid.
[3] Julie Cohen, 'Studying law studying surveillance' (2015) 13 Surveillance & Society 91, 99.

surveillance practices by 'reducing them to simple (and potentially regulable) observation and overlooking all of the ways in which they are productive.'[4] As a result, the law risks being premised on outdated concepts of surveillance that may well have been adequate for the protection of privacy in an earlier analogue era, but are no longer equal to the – more complex – challenges presented by the contemporary landscape.

Surveillance studies, on the other hand, unpacks surveillance practices to establish emerging cultures and themes impacting the individual and society which, in turn, enable traditional conceptions of surveillance to be questioned, diversified and refined accordingly. For example, over the past several decades, surveillance has progressed beyond a mere apparatus of the totalitarian state depicted by Orwell's *Nineteen-Eighty-Four* and Bentham's prison 'Panopticon.'[5] Contemporary surveillance has become more than this. In the digital age, the proliferation of Information and Communication Technologies ('ICTs') has led to such an explosion of personal data traffic that surveillance is now carried out by the corporation and ordinary citizen, as well as the state. For example: police can monitor social media to investigate and track a suspect; the corporation can surveil consumers' social media 'likes' or online shopping habits to influence future purchases; and, the individual can watch over their peers (on social media) or themselves via wearable health technologies (like the 'FitBit'). Society has therefore progressed beyond the Orwellian 'surveillance state,' where surveillance power rests in the hands of the government, to a culture of surveillance where ordinary citizens 'collude as never before in their own surveillance by sharing – whether willingly or wittingly, or not – their personal information in the online public domain.'[6] This democratisation of surveillance power in the digital age has inspired surveillance studies scholars to develop the definition of surveillance so that it encompasses the variety of different actors and purposes to which surveillance can now be put. Lyon, for example, defines surveillance as 'the operations and experiences of gathering and

[4] Cohen ibid 92.
[5] George Orwell, *Nineteen Eighty-Four* (First published 1949, Penguin, 2013); Jeremy Bentham, *The Panopticon writings (Ed. Miran Boovic)* (Radical Thinkers, 2010). See Chapter 3, Part 1, section 1.1 for discussion of Bentham's 'Panopticon.'
[6] Lyon (n 1) 12-13.

analysing personal data for influence, entitlement and management.'[7] In line with this broader approach to surveillance, this thesis defines surveillance as an exercise of 'watching over' 'in case of' something happening or the information 'one day' becoming useful. This definition is established in Chapter 1 via an historical analysis of surveillance in the UK.

A key theme in this thesis is the active participation by individuals in surveillance cultures.[8] This theme is registered and explored by the author's own concept of 'autobiographical surveillance' which is used to conceptualise individuals' performances on social media sites as a form of (self-) surveillance. This is achieved by characterising users' sharing on these platforms as a type of autobiography whereby real-life events, thoughts, and feelings (usually the most interesting or 'best bits') are transcribed into a prescribed, chronological, digital format that is then shared with a vast, mostly unseen audience. Key to characterising this practice as 'surveillance' is that social media users typically monitor their digital actions with an audience in mind and tailor their performances on these platforms accordingly. In other words, they internalise the gaze of other watchers – which is a well-accepted characteristic of surveillance.[9] Whilst the concept of 'self-surveillance' (and normative notions of the 'Quantified Self') exist in surveillance studies literature, my reworking of this concept goes beyond these by promoting the understanding of the individual's exposure online as a form of self-serving surveillance, as opposed to being perceived as antipathy toward privacy. The prefix 'autobiographical' not only captures the self-narration of

---

[7] Lyon, *The culture of surveillance* (n 1) 6.

[8] The theme of participation is increasingly evident in surveillance studies, see: Mark Andrejevic, 'The work of watching one another: lateral surveillance, risk, and governance' (2005) 2 Surveillance and Society 479; Paulo Vaz and Fernando Bruno, 'Types of Self-surveillance: from abnormality to individuals 'at risk'' (2003) 1 Surveillance and Society 272, 273; Anders Albrechtslund, 'Online social networking as participatory surveillance' (2008) 13(3) First Monday 1; Alice Marwick, 'The public domain: social surveillance in everyday life' (2012) 9 Surveillance and Society 378; Robert Tokunga, 'Social networking or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships' (2011) 27 Computers in Human Behaviour 705; Darin Barney, Gabriella Coleman, Christine Ross, Jonathan Sterne, Tamar Tembeck (eds), *The participatory condition* (University of Minnesota Press, 2015); Daniel Trottier, *Social media as surveillance*: *rethinking visibility in a converging world* (Ashgate publishing, 2012).

[9] 'Internalisation of the whips' developed in Michel Foucault, *Discipline and punish: the birth of the prison* (Penguin, 1991). Marwick also uses this argument to justify her conception of social media as surveillance in Marwick (n 8).

the individual who subscribes to the chronological documenting of their life in order to share with others, be watched and, in return, watch others; but also enables the sharing of personal information by others to be described as 'biographical.' This is used to demonstrate that we are not always the authors of our own digital narratives, with facts about ourselves being published online during the course of other users' autobiographies. This again is used to challenge the treatment of personal information and data online as 'fair game' or as an antipathy toward privacy.

By recognising activities like digital social networking as an expression of the individual's ownership of and responsibility for data exchange (and in turn, surveillance) it is possible for expectations of privacy to persist in realms of exposure, such as social media sites. Accordingly, it is important for the law to take into account these emerging themes and cultures in order to ensure that key legal doctrines (such as the reasonable expectation of privacy) retain relevance in the digital age. Therefore, this thesis contributes to bridging the gap between law and surveillance studies by using the latter to inform the law's understanding of the changed nature of the contemporary surveillance landscape. In doing so, the law can become more suited to the dynamic and fast-paced socio-technical landscape within which it attempts to intervene, re-configuring and extending the protection of privacy and safeguarding (and perhaps even enhancing) the benefits of ICTs and the cultures of surveillance that have emerged around them.

1 Thesis purpose, scope and concept

This thesis was inspired by National Security Agency ('NSA') sub-contractor Edward Snowden's disclosure of classified documents in 2013 which revealed 'suspicionless surveillance' carried out by intelligence agencies across the globe, although particularly by the American NSA and the UK's Government Communications Headquarters ('GCHQ'). The Snowden disclosures not only highlighted state overreach, but also the active role played by surveillance subjects.[10] Consequently, traditional conceptions of surveillance, such as Bentham's 'prison-panopticon,' which

[10] Lyon, *The culture of surveillance* (n 1) 8-10.

depicts the individual as a passive and powerless subject of state surveillance, are no longer adequate for conceptualising the modern surveillance landscape where the individual plays an active role in their own exposure (although, it should be noted that panopticism has been deemed inadequate for some time in surveillance studies literature).[11] This is especially true in the post-Snowden climate where individuals continue to facilitate - although not always enthusiastically or even consciously - mass surveillance practices via their performances online (particularly on 'Web 2.0' sites which rely on user-generated content, eg social media sites) and their engagement with ICTs. This is noted by Harcourt who argues in his work on the 'expository society' that:

> 'We are not forced; we *expose ourselves*. Rather than a surveillance apparatus stealthily and invasively forcing information out of us, more often than not we *exhibit ourselves* knowingly to that voyeuristic digital oligarchy – and we put ourselves at its mercy. We are confronted less with surveillance than with an oligarchical voyeur taking advantage of our exhibitionism.'[12]

Harcourt acknowledges that not all individuals contribute vociferously or actively to their 'data exhaust' (trails of data generated as a result of persons' online actions). However, it is reasonable to assume that most people at least generate some data as a by-product of life within modern society - whether it is 'with all our love' or 'anxiously and hesitantly.'[13] The alternative of going 'off grid' is made increasingly difficult by the interweaving of everyday life with the digital which, in turn, allows for the seepage of surveillance into the arteries and capillaries of culture.[14] Snowden's exposure (or

---

[11] Lyon argues that the panopticon is not incorrect but it is inadequate, in Lyon, *The culture of surveillance* (n 1) 8. Bentham's panopticon is examined in Chapter 3. Theories that move beyond the panopticon will also be examined in Chapter 3.
[12] Bernard Harcourt, *Exposed: desire and disobedience in the digital age* (Harvard University Press, 2015) 90.
[13] Ibid.
[14] Lyon *Surveillance after Snowden* (n 1) vi. The 'seepage of surveillance' is also depicted by Lyon and Bauman's theory on 'liquid surveillance' which refers to the spread of surveillance within the 'fluid and unsettling modernity of today,' in David Lyon and Zygmunt Bauman, *Liquid surveillance: a conversation* (Polity Press, 2013) 3.

highlighting) of these developments in the surveillance landscape calls for a reconsideration of conceptions and expectations underpinning surveillance laws as these may no longer be reflective of the environment within which they are now placed. The main research question of this thesis therefore asks whether UK surveillance law is suitable for the digital age? Suitability is assessed in terms of the law's protection of privacy which, as set out below, remains a highly valuable right within the digital era.

In answering the above research question, this thesis focusses on the major piece of UK surveillance legislation, the IP Act, and assesses its approach to the technocultural realities of the digital age. This is assessed in terms of the extent to which the Act recognises the following characteristics of the contemporary surveillance landscape: (i) the collapse of traditional dichotomies; (ii) the role of the individual; and (iii) the increased need for group privacy.

In carrying out this assessment, it is necessary to first establish: what is surveillance and how has it been impacted by the digitalisation of society? Chapter 1 therefore establishes the definition of surveillance via an historical survey of surveillance in the UK. This historical analysis also contributes to determining how the digital evolution has impacted surveillance by providing a benchmark for comparison with the contemporary surveillance landscape which is illustrated in Chapter 3. Chapter 3 adopts a theoretical approach by tracing the development of traditional theories of surveillance to new conceptions that take into account the impact of digital technologies on the surveillance landscape, namely: the collapse of traditional dichotomies; the additional role of the individual; and, increased risks for group privacy. Chapter 4 then goes on to establish the IP Act's approach to these characteristics of the contemporary surveillance landscape. Chapter 5 then assesses the suitability of this approach in terms of its protection of privacy under Article 8 ECHR. The definition of privacy will have already been defined under Article 8 ECHR in Chapter 2 (although reference is also made in this chapter to the CJEU's definition of

privacy in some of its recent surveillance case law which deals with the mass gathering of online communications).[15]

Following the above analysis, it is concluded that UK surveillance law does not provide adequate protection to privacy in the digital age as it fails to attune to the technocultural realities of the contemporary surveillance landscape. Chapter 6 subsequently concludes with recommendations aimed at enhancing the protection of privacy under the IP Act and, in turn, its suitability for the digital age.

Due to limited word count and the vastness of the subject matter, the scope of this thesis is restricted to the UK surveillance legal landscape and the definition of privacy according to the ECHR. Aside from the historical survey of surveillance in Chapter 1, which serves to provide context for subsequent discussion, this research primarily focusses on the post-Snowden period (2013 – present) as it is here that the evolution of the digital age and its impact on surveillance and privacy are particularly evident. Only certain aspects of this landscape that contribute to the overall argument of this thesis – that UK surveillance law does not adequately protect privacy due to its failure to understand the contemporary surveillance landscape - can be examined within the scope of this research. Three characteristics of this landscape are considered in depth: the collapse of dichotomies, the role of the individual, and risks to group privacy. In making this argument, only state surveillance (namely bulk state surveillance powers brought in under the IP Act) and non-vertical practices of surveillance (such as peer-to-peer and self-surveillance) are examined. Reference is made to corporate surveillance but only insofar as it is used by the state in advancing its own surveillance goals and demonstrating the hybridity of the contemporary surveillance landscape.

References to the 'individual' refer only to individuals in Western liberal democratic society where there exists almost universal access to ICTs. Consequently, the conclusions of this research are not necessarily transferable to countries where there is

[15] The main cases examined here are: Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd and Seitlinger v Minister for communications, marine and natural resources* [2015] EU:C:2015:650; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and others* [2016] EU:C:2016:970.

more restricted access to ICTs, or, where historical and cultural differences have impacted the way in which they are used.[16] Finally, whilst references are made in relation to individuals' participation in surveillance, it is acknowledged that not all individuals generate data to the same extent, if at all (although as noted above, it is increasingly difficult to avoid not generating *any* data in the digital age).

2 The value of privacy

The importance of this research lies in the continued value of privacy in the digital age. This thesis defines privacy according to Article 8 of the ECHR in Chapter 2. This definition is then used to critically assess the IP Act's approach to the contemporary surveillance landscape. Therefore, privacy is central to the purpose of this research which will, ultimately, make recommendations as to how this right could be better protected in the digital age. It is thus necessary to establish the value of privacy.

2.1 Approaching privacy

There exists a vast body of literature examining the value of privacy that has been reinvigorated post-Snowden as a means of critiquing new surveillance technologies and practices. Whilst the digital landscape has also fostered the 'privacy is dead' rhetoric, calls for the consignment of privacy to the history books are dwarfed by literature underlining its fundamental importance to individuals and liberal-democratic society.[17]

Various works on privacy state the definitional issues that surround it and the subsequent challenge in locating and conveying its value. Bennett, for example, notes

[16] For example, in Germany there is a strong distrust for government surveillance due to its history of dictatorship which has resulted in Germans being especially concerned about their privacy which has resulted in strong data protection laws and potential differences in how individuals engage online. See Stefan Heuman, 'German exceptionalism? The debate about the German Foreign Intelligence Service (BND)' in Russell Miller (ed) *Privacy and power: a transatlantic dialogue in the shadow of the NSA affair* (Cambridge University Press, 2017).

[17] Mark Zuckerberg, Facebook founder, speaking at the Crunchie awards in San Francisco (*Guardian news*, 11 January 2010) <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> accessed 5 September 2016.

that 'attempts to define the concept of 'privacy' have generally not been met with any success.'[18] Similarly, Solove describes privacy as

> '[a] concept in disarray…a sweeping concept, encompassing (among other things), freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection from one's reputation, and protection from searches and interrogations.'[19]

Therefore, it is best to function on 'an understanding of privacy as an umbrella term that encompasses a variety of related things.'[20]

Clarke was the first to develop a typology categorising different types of privacy. This included the privacy of: the person; behaviour; data; and, communication.[21] Finn et al and Raab and Wright have since expanded this list to include other types of privacy, such as thoughts and feelings, location and space, and association.[22] As shown in Chapter 2, a pluralistic approach to privacy is also taken by the European Court of Human Rights ('ECtHR') which has consistently defined 'private life' as a 'broad term not susceptible to exhaustive definition.'[23] This has, in turn, enabled Article 8 to

---

[18] Colin Bennett, *Regulating privacy: data protection and public policy in Europe and the United States* (Cornell University Press, 1992) 25.
[19] Daniel Solove *Understanding Privacy* (Harvard University Press, 2008) 1. See also, Ferdinand David Schoeman, *Philosophical dimensions of privacy: an anthology* (Cambridge University Press, 1984) 444.
[20] Neil Richards, Intellectual privacy: rethinking civil liberties in the digital age (Oxford, 2015) 9.
[21] Roger Clarke, 'Introduction to dataveillance and information privacy, and definition in terms' (*Roger Clarke's homepage*) <http://www.rogerclarke.com/DV/Intro.html> accessed 14 June 2018.
[22] Rachel Finn, David Wright, and Michael Friedwald list seven types of privacy in, 'Seven types of privacy' in Serge Gutwirth, Ronald Leenes, Paul de Hert, Yves Poullet (eds) *European data protection: coming of age* (Springer, 2013). Wright and Raab add to these seven types of privacy with 'other types of privacy' in David Wright and Charles Raab, 'Privacy principles, risks, and harms' (2014) 28 International Review of Law, Computers & Technology 277. Solove also develops a taxonomy of privacy in Solove (n 19) 9. Nissenbaum argues that privacy's value is context dependent, see Helen Nissenbaum 'Privacy as contextual integrity' (2004) 79 Washington Law Review 119, and *Privacy in context: technology, policy, and the integrity of social life*' (Stanford University Press, 2010).
[23] *Niemietz v Germany* (1996) 16 ECHR 97, para 29; *Peck v United Kingdom* (2003) 36 ECHR 41, para 57; *Pretty v United Kingdom* (2002) 35 ECHR 1, para 61.

provide a broad platform for a variety of different complaints that might otherwise fail to engage the ECHR.

The growing preference for privacy to be understood as a pluralistic value leads Solove to criticise attempts at identifying a single, intrinsic, value of privacy as abstract and failing to go beyond describing it as a 'mere taste.'[24] In agreement, the following provides an overview of the individual and social values of privacy as means of underlining the continued importance of privacy in the digital age and, in turn, the importance of this research.

2.2 The individual value of privacy

The value of privacy is often described in terms of its functional value to autonomy, freedom, and personhood. Rossler, for example, explains that:

> '[a]s a condition for autonomous decisions and the ensuing autonomous life and behaviour there are certain forms of one's practical self-relationship – reflections on conflicting desires and self-images, on the genesis of desires etc. – that can only be successfully developed if there are protected private realms and dimensions in one's life.'[25]

Thus, privacy grants space to the individual where he or she is free from the gaze of others – or what Westin describes as the 'whirlpool of active life'[26] - enabling them to explore and develop a sense of self and to enjoy 'the individual freedom exacted and legally safeguarded in modern societies.'[27] Privacy might, therefore, be viewed as something of a gateway right that facilitates the individual's enjoyment of other rights and freedoms characteristic of liberal-democratic society. This is supported by Westin

[24] Solove (n 19) 84.
[25] Beate Rossler, *The value of privacy* (Polity Press, 2005) 72.
[26] Alan Westin, *Privacy and freedom* (Ig publishing, 2015) 35.
[27] Rossler (n 25) 72.

who underlines the role of privacy in the promotion of freedom of association, expression, the press, and the protection of the voting process.[28]

In addition, privacy allows for self-disclosure as the individual is able to choose when, how, if, and to whom they wish to reveal aspects of their lives. This, in turn, facilitates the development of (intimate) relationships that, Rosen argues, are dependent upon 'slow mutual self-disclosure.'[29] It follows that, without privacy, everything would be available to everyone and there would be such a suffocating degree of openness that opportunities for intimacy would be stifled. Thus, privacy is also intrinsic to sociality.

Whilst the above values of privacy are integral to the individual's enjoyment of a free and autonomous life, they are also crucial to democratic society as a whole. However, the societal interest in privacy struggles to find expression in frameworks that are rooted in the individual rights model. As a result, group privacy is typically only recognised in terms of an aggregation of individual privacy interests as opposed to being regarded autonomously (as shown in Chapter 2). This is acknowledged in Bennett and Raab's work on the conventional 'privacy paradigm' discussed below.[30]

2.3 The social value of privacy

Whilst the individual value of privacy is evident and well covered in the academic literature, privacy scholars warn against an over-emphasis on the individualistic properties of privacy because it risks placing privacy in conflict with the common good.[31] Therefore, it is important to contextualise the individual value of privacy through an analysis of its societal value. For example, by providing the individual with a sanctuary from society's gaze, it enables fledgling beliefs and opinions to be nurtured into well reasoned fully-formed arguments which, once developed, can be offered up

[28] Westin (n 26) 25.
[29] Jeffrey Rosen, *The unwanted gaze: the destruction of privacy in America* (Vintage Books, 2000) 8-9.
[30] Colin Bennett and Charles Raab, *The governance of privacy: policy instruments in global perspective* (MIT Press, 2006) 44.
[31] Benjamin Goold, 'Surveillance and the political value of privacy' (2009) 1 Amsterdam Law Forum 3.

for democratic deliberation.[32] Thus, without privacy, views and opinions risk being 'prematurely leaked to the world, where harsh judgements might crush them,' potentially debilitating societal progression.[33] Boone also argues that it is not only in the development of the individual that privacy supports democratic society as it also 'underwrites the freedom to vote and hold political discussions, and to associate freely away from the glare of the public eye and without fear of reprisal.'[34] Therefore, 'whilst democracy is incompatible with isolation; it can, however, flourish where privacy exists.'[35]

Bennett and Raab's illustration of the 'privacy paradigm' is especially effective in capturing the importance of recognising the societal value of privacy.[36] The 'privacy paradigm' is a set of interrelated assumptions about the public and the private.[37] It rests on the assumption that society is comprised of relatively autonomous individuals and that society is no more than the sum total of these individuals (which the authors describe as an 'atomistic conception of civil society').[38] Individuals are positioned as the best judges of their own privacy, the value of which may vary from person to person.[39] Bennett and Raab argue that this conventional privacy paradigm underpins the modern claim to privacy. Consequently, privacy protections are typically framed individualistically and aimed at protecting the individual's right to 'be let alone' from other individuals, organisations and agencies.[40] However, upon review of privacy and surveillance, the authors consider whether a less atomistic approach to liberal-democratic society should be adopted so that privacy's societal value is able to

[32] See Paul Schwartz, 'Privacy and democracy in cyberspace' (1999) 52 Vanderbilt Law Review 1609.
[33] Solove (n 19).
[34] Keith Boone, 'Privacy and community' (1983) 9 Theory and Social Practice 1, 8.
[35] Charles Raab, 'Privacy, democracy, information' in Brian Loader (ed) *The Governance of cyberspace: politics, technology and global restructuring* (Routledge, 1997) 157.
[36] Bennett and Raab (n 30).
[37] Ibid 4.
[38] Ibid.
[39] Ibid. Westin demonstrates how different cultures can impact individuals' value of privacy, see Westin (n 26) 26-27.
[40] Ibid. This is in line with Warren and Brandeis' concept of privacy as the 'right to be let alone' in Samuel Warren and Louis Brandeis, 'The right to privacy' (1890) 4 Harvard Law Review 193.

transcend the interests of the individual (albeit not to the detriment of the latter).[41] They conclude that:

> 'individual privacy is only truly achievable in a society in which privacy is considered socially valuable and which reflects that esteem in its collective decision-making – in other words, in its political and governmental activity.'[42]

However, not all scholars agree on the societal value of privacy. Etzioni, for example, adopts a communitarian approach by arguing that privacy can act as 'a societal license that exempts a category of acts…from communal, public, and governmental scrutiny.'[43] In doing so, he constructs privacy as a shield for wrongdoing and an obstacle to security that enables regression from the public sphere and allows transgressions to occur in secret. Thus, privacy according to Etzioni obstructs social control and delays changes to norms. In response, he proposes a 'new communitarian concept of privacy' aimed at balancing privacy and the common good on the basis that privacy (as with other principles and values) is not always fully compatible with societal concerns.[44] However, how such a balance might be reached and by whom is unclear.

Solove's interrogation of Etzioni's approach through an examination of blackmail law during the Victorian era is especially useful in identifying the flaws in his argument.[45] During this period, sodomy was illegal and harshly punished. Consequently, when upper-class men engaged in homosexual acts with prostitutes or men from the lower classes, they frequently became victim to blackmail.[46] However, instead of re-considering the social norms condemning sodomy, strict blackmail laws were enacted. Solove acknowledges that, in this sense, privacy may be seen as enabling society to 'maintain the fiction that its norms are being followed while deviant conduct is hidden

---

[41] Bennett and Raab (n 30) 44.
[42] Ibid.
[43] Amitai Etzioni, *The limits of privacy* (Basic Books, 1999) 196.
[44] Ibid, at 15 and 200.
[45] Solove (n 19).
[46] Ibid.

behind the veneer.'[47] However, this construction of privacy as concealment is problematic in its creation of a rigid dichotomy between privacy and the collective good. This dichotomy serves to conceal the fact that privacy also offered invaluable protection to homosexual men against

> 'the tyranny of the prevailing opinion and feeling; against the tendency of society to impose, by other means than civil penalties, its own ideas and practices as rules of conduct on those who dissent from them.'[48]

In offering this protection, privacy allowed men to explore and investigate feelings that were condemned by society as 'immoral' and 'wrong' and, in turn, develop arguments in defence of them. Once ready, these arguments could then be used to challenge the status quo, invoke change, and inspire societal progression.

The above notion of privacy as concealment has also found expression in other theories and contexts, some of which pose significant challenges to the value of privacy as a societal good. Some feminists, for example, have critiqued privacy as a mechanism of control and repression used by men to crystallise their position in the public realm, to expel women to the domestic sphere and to conceal issues therein (such as domestic abuse).[49] Allen and Mack criticise Warren and Brandeis' concept of privacy as the right to be let alone for over-emphasising privacy as seclusion and failing to interrogate the ways in which this impacts women's enjoyment of the right to privacy.[50] Mackinnon goes as far as calling for a collapse of the private realm in order to render everything public and, therefore, free women from the encasement that is the home.[51] Although, Gavison and Olsen question the desirability of this proposal, warning of an alternative system 'in which the state controls every aspect of human life and nothing

---

[47] Ibid.
[48] John Stuart Mill, *On Liberty* (Digireads.com, 2010) 9.
[49] Catharine MacKinnon, *Toward a feminist theory of the state*, (Harvard University Press, 1989); Susan Moller Okin, *Justice, gender and the family* (Basic Books, 1989); Ruth Gavison, 'Feminism and the public-private distinction' (1992) 45 Stanford Law Review 1; Anita Allen and Erin Mack, 'How privacy got its gender' (1990) 10 Northern Illinois University Law Review 441.
[50] Allen and Mack ibid 477.
[51] MacKinnon (n 49).

is personal or private.'[52] Thus, whilst there exists concern over the public-private divide and an acceptance that boundaries between the two might need to be re-drawn to empower women, it is more widely accepted that the value of privacy prevails in protecting against unjustified state intervention and creating spaces free from the governmental gaze. Privacy should not, therefore, be rejected in an attempt to resolve issues of gender inequality.[53]

Privacy as concealment is also evident in the national security context where it is frequently portrayed as something of an obstacle or hindrance to security on the basis that it enables those who have something to fear, to hide. The 'nothing to hide' argument is typically used in response to privacy concerns raised over state surveillance and poses a particularly difficult obstacle for privacy advocates to overcome because, despite being deeply flawed, the simplicity of the argument does well to garner popular support. Also, arguments stating privacy's value are comparatively less emotive and simplistic than the 'nothing to hide' argument. As Goold notes, 'explaining why privacy is important in terms that a lay member of the public is likely to engage with is difficult, mostly because privacy is an inherently complex concept.'[54]

However, the 'nothing to hide' argument is premised on an overly narrow and simplistic construction of privacy as a highly individualistic right that distorts its social and political value.[55] Consequently, when placed in opposition to a value like 'security' which is more readily associated with the common good (despite also being a 'promiscuous concept'), the balance is skewed towards the protection of the so-called 'collective' value and privacy is left to be enjoyed as something of a luxury when not

---

[52] Frances Olsen, 'The family and the market: a study of ideology and legal reform' (1983) 96 Harvard Law Review 1497, 83. Gavison (n 49) 28-29.
[53] See Judith Wagner Decew, 'The feminist critique of privacy' in Beatte Rossler, Dorota Mokrosinska (eds) *Social dimensions of privacy* (2015) 92-94.
[54] Goold (n 31) 3.
[55] Regan similarly described the opposition between privacy and security as 'simplistic,' as it fails to acknowledge the complexity of public and private relationships in Priscilla Regan, *Legislating for privacy: technology, social values, and public policy* (University of North Caroline Press, 1995) 217

in opposition to the common good.[56] In addition, Raab argues that the positioning of privacy in conflict with security serves to overlook the affinity that exists between the two with privacy often involving

> 'protective, defensive and risk-averse measures in the service of privacy, autonomy, dignity, and sociality in the face of technologically assisted policy initiatives in a society driven by counter-terrorism, law-enforcement, and a preoccupation with personal safety.'[57]

Raab thus constructs privacy as another 'take' on security as opposed to it being constituted as a conflicting value. This challenges calls like Etzioni's for a balancing or trade off between the two.[58]

Whilst the 'nothing to hide' argument demonstrates the ease with which privacy can be reduced to such an extreme individualistic level, this is 'not an argument for abandoning it.'[59] Nissenbaum goes as far as arguing that although 'individual interests in privacy are not irrelevant, they should be secondary considerations to 'those moral and political values that privacy is presumed to support.'[60] In agreement with Bennett and Raab, Lyon and Nissenbaum call for greater recognition of privacy's societal value. As will be shown in this thesis, support for this approach has grown in response to the unfolding technological landscape,

---

[56] Security as a 'promiscuous concept' from Lucia Zedner, *Security* (Routledge, 2009) 9. Raab also notes that 'to ignore the perception that privacy is *also* a collective citizen interest is to put a thumb on the 'balancing' scale,' as well as influencing how the public view and understand the value of privacy, in Charles Raab, 'Security, privacy and oversight' in Andrew Neal, *Security in a small nation* (Open Book Publishers, 2017) 88.

[57] Charles Raab, 'Privacy as a security value' in Schartum et al (eds) *Jon Bing: en hyllest/a tribute* (Gyledendal, 2014) 55.

[58] Ibid 56. The RUSI report published in the aftermath of the Snowden disclosures also challenged the dichotomy between privacy and security, noting that: 'A common and repeated assumption made by politicians, the media and the general public is that these values are opposed, and that the issue is one of "national security" versus "personal privacy,"' in Royal United Services Institute for Defence and Security Studies, *A democratic license to operate: report of the independent surveillance review* (RUSI, 2015), p 16.

[59] Lyon Surveillance after Snowden (n 1).

[60] Ibid 73.

> 'where risks relating to the use of big data may play out on the collective level, and where personal data is at one end of a long spectrum of targets that may need consideration and protection.'[61]

In light of this reality, this thesis calls for the development of a group privacy right under Article 8 ECHR that shifts the focus away from the individual in cases concerning mass, data-driven surveillance.

2.4 Summary

From the above overview, it is evident that ascribing a single, abstract value to privacy is neither possible nor constructive. Instead, it needs to be viewed pluralistically.[62] Whilst privacy's individual value is paramount, it is important that privacy is also understood as a common good so that it is suitably positioned among other rights and values, like security. Failing to do so leaves privacy vulnerable to manipulation and characterisation as a 'disease' plaguing 'effective active government – government that innovates, that protects people who need protecting, that acts aggressively when action is needed.'[63] This view is inherently problematic as it bastardises a right that is intended to be enjoyed as an intrinsic virtue of being human, that is integral to living as a free and autonomous human, and transforms it into a shield for wrongdoing. Under this rhetoric, the surrender of privacy comes to be celebrated as a badge of honourable citizenship or as testament to one's innocence. This thesis therefore endorses privacy as an individual and societal value that has not been displaced in the digital age.

3 Original contribution to knowledge

This thesis makes an original contribution to knowledge by providing unique critical analysis on the protection of privacy under the IP Act in the digital age. The multidisciplinary approach combining legal, sociological, and surveillance studies

---

[61] Linnett Taylor, Luciano Floridi, Bart van der Sloot, 'Introduction: a new perspective on privacy' in Linnett Taylor, Luciano Floridi, Bart van der Sloot (eds) *Group Privacy: new challenges of data technologies* (Springer, 2017) 1.
[62] As as also concluded by Solove in Daniel Solove, '"I've got nothing to hide" and other misunderstandings of privacy' (2008) 44 San Diego Law Review 745, 763.
[63] William Stuntz, 'Secret service: against privacy and transparency' (2006) 234 New Republic 12, 12.

offers a novel reading of privacy in the context of the contemporary surveillance landscape. It also underlines the importance of the law's understanding of this environment to preserve privacy in the digital age. The author's original concept of 'autobiographical surveillance' also offers a novel development of existing theories of self-surveillance to illustrate the benefits of surveillance bestowed on civil society by the contemporary surveillance landscape and the need to protect them.

4 Thesis structure

This thesis is divided into six chapters.

Chapter 1 provides context for subsequent discussion by carrying out an historical survey of surveillance in the UK, illustrating the surveillance landscape prior to its digitalisation in the 21st century. In doing so, this chapter contributes to establishing what impact the digitalisation of society has had on the surveillance landscape. As well as providing background, this chapter also serves a definitional purpose by identifying the key characteristics of surveillance and distinguishing it from pure information gathering practices. This chapter is largely chronological and adopts a thematic structure to illustrate the different uses of surveillance and the peaks and troughs with which it has typically been used across different contexts and eras. This chapter also demonstrates that the legal regulation of surveillance has struggled to develop in the UK resulting in periods of legislative lag.

Chapter 2 serves a definitional purpose, defining privacy in terms of the ECtHR's application of Article 8 ECHR (mostly in its surveillance jurisprudence). In doing so, this chapter provides a benchmark against which the IP Act's impact on privacy is critically assessed in Chapter 5. For the purposes of clarity, this chapter adopts the structure of the ECtHR's assessment of interferences with Article 8, thus examining: (i) the engagement of the right by surveillance practices; (ii) the legality of interferences; (iii) the justifiability of interferences. Potential limitations in Article 8's protection of privacy within the contemporary surveillance landscape are also considered via a comparison of the approaches taken by the ECtHR and the Court of Justice of the European Union ('CJEU') in the determination of discretion and proportionality in surveillance cases. Finally, in light of the aforementioned societal

value of privacy, this chapter examines the scope for an autonomous group privacy right to be enjoyed under Article 8.

After having covered the necessary definitional and contextual discussion in Chapters 1 and 2, Chapter 3 illustrates the contemporary surveillance landscape. This chapter therefore establishes the impact of the digital evolution on the surveillance landscape. A theoretical approach is adopted with various conceptualisations of surveillance being used to depict the hybrid and dynamic nature of the modern surveillance reality. The chapter is structured according to three 'waves' of surveillance theory: (i) the panopticon and panopticism (ii) post-panoptical theories, and (iii) new conceptualisations of surveillance. This structure was inspired by Galic et al's work on the 'phases' of surveillance theory with each phase representing a shift or development in surveillance theory (for example, from disciplinary to controlling to entertaining conceptions of surveillance).[64] The third wave reflects the contemporary surveillance landscape which is illustrated via an examination of smartphones and social media as 'sites of third wave surveillance.' It is here that the author's own theory of 'autobiographical surveillance' is introduced. This chapter concludes by identifying the following legal implications of the third and current wave of surveillance: (i) participation of the individual; (ii) collapsing dichotomies; and, (iii) a need for group privacy. These implications will provide the basis for analysis of the UK surveillance legal landscape in Chapters 4 and 5.

Chapter 4 establishes the UK's approach to the contemporary surveillance landscape. This is achieved via an examination of the IP Act's response to the legal implications of the third wave identified in Chapter 3. First, in determining its response to the collapse of dichotomies, distinctions maintained in the Act are examined in terms of their relevancy and viability in the digital age. Second, bulk data-focussed surveillance powers are examined to demonstrate the positioning of participation under the Act. From this, it is established that the Act has adopted a 'needle-in-the-haystack'

[64] Galic et al, 'Bentham, Deleuze and beyond: An overview of surveillance theories from the Panopticon to participation' (2017) 30 Philosophy of Technology 9; Galic et al, 'Surveillance theory and its implications for law' in Roger Brownsword, Eloise Scotford, Karen Yeung (eds), *Routledge handbook of the law and regulation of technology* (Edward Elgar Publishing, 2017).

approach to the increased participation of the individual in surveillance. It is argued that this poses considerable risks to the individual's privacy and enjoyment of surveillance. Third, the bulk powers in the IP Act are used to illustrate the need for a group privacy right under Article 8 ECHR which, it is argued, maintains an overly individualistic focus in the face of increasingly mass, un-targeted surveillance practices.

Chapter 5 assesses the impact of the IP Act's approach to the contemporary surveillance landscape on the protection of privacy under Article 8 ECHR. First, the impact of the 'haystack-needle' approach is considered via an examination of the bulk, data-focussed powers in the IP Act under Article 8. The questionable proportionality of these powers is used to illustrate the failure to properly position the participation of the individual under the IP Act. Second, the IP Act's failure to recognise the collapse of dichotomies is examined via an analysis of safeguards determined on the basis of outdated distinctions maintained in the IP Act (namely the distinction between communications 'content' and 'data'). Whilst the ECHR provides a safety net to some of the practices slipping through the IP Act, it is also shown that the ECtHR needs to develop its approach in surveillance cases in order to reflect the different harms to privacy emerging from the contemporary surveillance landscape. On the basis of this analysis, Chapter 5 concludes that the IP Act fails to provide adequate protection to privacy in the digital age due to a failure to attune to the technocultural realities of the contemporary surveillance landscape.

Chapter 6 makes recommendations as to how the IP Act can enhance its protection of privacy. These are aimed at improving the Act's response to the technocultural realities of the digital age. Recommendations are thus made as to how to: (i) re-construct traditional boundaries; (ii) re-position the participation of the individual; and, (iii) recognise the privacy of the group. Before making these recommendations, the chapter begins with an analysis of the role of law in cyberspace. This is to ensure that the recommendations made are reflective of the reality for which they are intended to be implemented. Three main regulatory models for the internet are considered: (i) cyberlibertarianism; (ii) cyberpaternalism; and, (iii) network communitarianism. Endorsing a network communitarian approach on the basis that it best acknowledges

the role of the individual in the regulatory process, recommendations are made that are aimed at harnessing this approach. The recommendations made in this chapter thus focus on enhancing the legitimacy of the law in the eyes of its regulatees by, for example, re-conceptualising privacy so that it is more reflective of individuals' expectations of privacy in the contemporary landscape. It is argued that, in doing so, they will be 'pulled to compliance' and a more productive regulatory intervention can be made.[65] Recommendations also underline the need for the law to engage with other disciplines and for non-legal regulatory tools to be used so that a more dynamic and hybrid regulation of surveillance can be established. After having made recommendations for change, this thesis concludes with suggestions for future research, a thesis summary, and concluding remarks.

[65] 'Pull to compliance' taken from Thomas Franck in, 'Legitimacy in the international system' (1988) 82 American Journal of International Law 705.

Chapter 1 A history of surveillance in the UK

Introduction

This chapter serves a scene-setting function by providing an historical analysis of surveillance in the UK. In doing so, this chapter contributes to establishing the impact of the digital evolution on the surveillance landscape. This chapter also serves a definitional purpose by establishing when information gathering ends and 'surveillance' begins. In doing so, this chapter enables continuities and deviances in the contemporary surveillance landscape to be identified in Chapter 3. The IP Act's response to these developments are subsequently identified in Chapter 4 and critically assessed in Chapter 5.

The historical analysis in this chapter illustrates the peaks and troughs with which surveillance has been used in the UK. It can subsequently be demonstrated whether the current breadth of powers in the IP Act are typical for present circumstances or represent an exceptional level of surveillance. This will contribute to the critical analysis of the IP Act in terms of its suitability in the digital age. These peaks and troughs are showcased by the thematic approach of this chapter. The following themes are used to illustrate the varying uses of surveillance across different contexts and epochs: (i) taxation and social welfare; (ii) crime and disorder; (iii) war; and, (iv) national security. These contexts have been selected on the basis that they illustrate the multi-faceted functions and purposes to which surveillance can be put.

This chapter also provides a benchmark against which the contemporary surveillance landscape can be analysed. In doing so, developments in surveillance that have been brought about by the digitalisation of society can be identified, such as the additional role of the individual. In turn, the approach taken by the IP Act towards these developments can be assessed and its impact on privacy critically analysed. The current chapter largely excludes the 21st century from its analysis as this period is reserved for Chapter 3's analysis of the contemporary surveillance landscape. The 11th century has been chosen as the start point as it is here that the first nation-wide information gathering practice occurred with 'The Book of Domesday.'

1 Definitions of surveillance

There is an array of definitions for surveillance. The word 'surveillance' comes from the French verb 'surveiller' which means 'to watch over.' However, this broad definition is limited in use as it could include a number of activities that would not naturally be considered 'surveillance,' such as a mother 'watching over' her child in a park. The Cambridge dictionary provides a much narrower definition: 'the careful watching of a person or place, especially by the police or army, because of a crime that has happened or is expected.'[66] However, this definition excludes practices that should rightly be classified as surveillance, such as the mass surveillance of communications in the criminal justice context without any suspicion, or even expectation, of wrongdoing by the vast majority of individuals.

David Lyon provides something of a happy medium by defining surveillance as 'the focused, systematic and routine attention to personal details for purposes of influence, management, protection, or direction.'[67] However, he notes that a number of exceptions to this definition now exist in the contemporary surveillance landscape where there is not always focused, systematic or routine attention to a particular individual.[68] In light of these definitional issues, the historical analysis of this chapter helps to identify the points at which pure information gathering practices become surveillant in nature. Drawing on the above definitions, this thesis understands surveillance to occur when there is a 'watching over' 'in case of' something occurring or information 'one day' become useful. This is as opposed to every morsel of information being used for a specific purpose which, as shown below, is the case for pure information gathering practices.

2 Contexts of surveillance

This section examines the history of surveillance under each of the aforementioned themes: (i) taxation and social welfare; (ii) crime and disorder; (iii) war; and, (iv)

---

[66] Cambridge dictionary online <https://dictionary.cambridge.org/dictionary/english/surveillance> accessed 27 March 2018.
[67] David Lyon, *Surveillance studies: an overview* (Polity Press, 2007) 14.
[68] Ibid.

national security. These themes represent typical contexts of surveillance and thus provide a good starting point for discussion. They also show where more intense surveillance has been deemed necessary and acceptable (eg in times of emergency and war), and where surveillance has been deemed too much and there has been push-back by the courts. Establishing these points will help to later analyse deviances in the contemporary surveillance landscape. Finally, as stated above, by tracing the historical waves with which surveillance has traditionally been used, a benchmark is provided against which developments in the contemporary surveillance landscape can be identified and subsequently used as the basis for assessing the suitability of the IP Act in the digital age.

2.1 Taxation and social welfare

The following contributes to defining surveillance by demonstrating the distinction between information gathering and surveillance practices in the context of tax and social welfare. The first section focuses on pure information gathering practices, such as 'The Book of Domesday' where only information that was absolutely necessary for the stated purpose was gathered. A distinction is subsequently drawn between information gathering and surveillance via the second subsection on the administration of the poor. Here is it shown that information was gathered in order to manage, control, and discipline the vagrant and impoverished (in anticipation of some consequential, future action), as opposed to just establishing facts on those living in poverty.

2.1.1 Information gathering

State information gathering in the UK can be seen from as early as the 11th Century under William the Conqueror.[69] In 1085, William ordered the collation of information on each of the English manors under the direction of the monks.[70] The task was eventually finished in the year of William's death in 1087 and was called, 'The Book of Domesday.' It remains one of the most famous English public records to date.[71]

[69] Sally Harvey, *Domesday: Book of Judgment* (Oxford University Press, 2014).
[70] Edward Higgs, *The Information State in England* (Palgrave Macmillan, 2004) 2.
[71] Henry Clifford Darby, *Domesday Economy* (Paperback edn University of Cambridge, 1986) ix.

It is widely agreed that the book served taxation purposes, although due to it being a one-off exercise and its omission of entire areas it is considered limited in terms of its usefulness.[72] It also only collected information on the manors, thus neglecting to take into account the rest of the population.[73] However, in light of its specific taxation purpose, the manors arguably bore most relevance to the exercise.

In 1801 a more comprehensive attempt at public record making was made with the first decennial census being carried out across England, Scotland, and Wales.[74] The census was implemented under John Rickman following the publication by Thomas Malthus of 'An Essay on the Principle of Population'[75] in 1798 which argued that the 'population, when unchecked, increased in a geometrical ratio. Subsistence increased only in an arithmetical ratio.'[76]

Rickman's censuses are now largely regarded as 'headcounts, rather than nominal censuses' due to the limited individual-specific information they included.[77] It was not until The Population Act 1840 which prescribed the inclusion of: name, age, sex, occupation, relationship to the head of the household, and country of birth, that the collected data was capable of being searched for information on a specific individual. Although, the searching of records was such a costly and labour-intensive task that it was rarely undertaken.[78]

The increased regulation of previously unchartered areas of the state developed a growing need for fast and easy ways to check individuals' credentials. For example, the regulation of the working age under the Factory and Workshop Act 1891 created a requirement for employers to confirm the ages of their employees. This led to the proliferation of birth certificates and their central storage by the General Registry

---

[72] Darby ibid 57.
[73] Ibid 57-61.
[74] An Act for Taking an Account of the Population of Great Britain, and of the Increase or Diminution thereof 1800.
[75] Thomas Malthus, An Essay on the Principle of Population, as it Affects the Future Improvement of Society with Remarks on the Speculations of Mr. Godwin, M. Condorcet, and Other Writers (First printed 1798, Electronic Scholarly Publishing Project 1998).
[76] Ibid 4.
[77] Higgs (n 70) 72.
[78] Ibid 73.

Office ('GRO') for ease of cross-checking.[79] Social reform legislation thus served to motivate the implementation of a more efficient system of information gathering and storage in order to facilitate and monitor adherence to the new laws. The centralisation of information gathering and storage practices may, therefore, be seen as beneficial to the individual by helping enforce laws aimed at the protection of their rights and interests.

The above examples provide an illustration of what this thesis means by 'information gathering' - a benign technique used for the effective administration of the state and the purpose for which has been disclosed to the individual. Surveillance, on the other hand, is never either entirely benign or malign, nor is it ever neutral.[80] This will be illustrated further in the following discussion. Furthermore, unlike the Book of Domesday where information was only gathered that was absolutely necessary for achieving the aim, surveillance involves an element of contingency with information being gathered 'in case of' it becoming useful as opposed to it being absolutely necessary for a stated purpose (eg a phone call being intercepted 'in case of' a criminal plot being revealed).

2.1.2 Administration of the poor

Following the Act of Supremacy 1534 declaring King Henry VIII as the Supreme Head of the Church of England, England was effectively severed from papal authority in Rome.[81] The ensuing dissolution of the monasteries between 1530 and 1560 effectively removed the institutions that had traditionally helped those who no longer had anywhere to turn for respite or support.[82] Consequently, in the face of social unrest and growing unemployment, Elizabeth I passed 'The Act for the Relief of the Poor 1601' (referred to as 'The Old Poor Law').[83]

---

[79] Factory and Workshop Act 1891, s 20.
[80] Lyon, Surveillance studies: an overview (n 67) 96.
[81] Act of Supremacy 1534, s 1.
[82] Paul Slack, Poverty and Policy in Tudor and Stuart England (Longman, 1988).
[83] Poor Law Act 1535, s 12.

The Old Poor Law formalised the prior system for poor relief and placed the responsibility of the destitute in the hands of local parishes[84] by imposing a compulsory poor rate on parish householders.[85] The law also established the creation of 'overseers of the poor' who administered the money, clothing, and food given to the poor. The system relied heavily on the creation and maintenance of extensive records by overseers and parish officials who detailed the relief received by individuals.[86] These records were then published to local communities to enable the close examination of recipients,[87] effectively creating 'a system of surveillance to weed out the "unworthy."'[88] Those deemed 'undeserving' of poor relief (ie those capable of working) could have their relief removed and be returned to their own local parish to work.[89] Unlike the examples of pure information gathering provided in the previous section, the rigorous information gathering on and close examination of the poor clearly shifts more towards surveillance, with information providing a basis for elite judgment and evaluation of the individual. In support of this, Higgs argues that 'the workings of the old Poor Law generated some of the most rigorous forms of information-based surveillance.'[90]

In the early 1830s there was an eruption of public outrage over climbing tax rates caused by rising bread prices and family sizes which eventually resulted in the impugnment of the existing poor relief system.[91] Following a Royal Commission report on the state of poor law administration in 1834, it was agreed that reform was necessary.[92] Adopting the Commission's conclusion that the poor relief system was being abused by those able to work,[93] the 1834 Poor Law Amendment Act ('the New Poor Law') was passed which overhauled the existing poor relief system and restricted

[84] The Old Poor Law consolidated previous Acts including the Vagabonds Act 1572 and the Act for the Relief of the Poor 1597
[85] 1601 Act, s 1.
[86] Ibid
[87] Higgs (n 70) 41.
[88] Ibid 41.
[89] Ibid.
[90] Ibid 40.
[91] Derek Fraser, *The Evolution of the British Welfare State* (2nd edn, Palgrave Macmillan, 1984), 36.
[92] Royal Commission, Report from his Majesty's Commissioners for Inquiring into the Administration and Practical Operation of the Poor Laws (C (1_{st} series) 44, 1834).
[93] Ibid 9.

its beneficiaries to the old and sick – otherwise considered the 'deserving poor.'[94] The 1834 Act thus further centralised the administration of the poor, shifting more control to central government and away from local parishes.[95] In turn, the poor were subjected to greater bureaucratic techniques to ensure stricter state monitoring of the poor law accounts.[96]

The centralisation of the administration of the poor under the 1834 Act encouraged a widespread culture of recording, classifying and monitoring of the poor which continues to be seen today.[97] However, with the digitalisation of records, more discreet techniques can be used to monitor the welfare system and investigate suspects of benefit fraud. For example, the IP Act enables public authorities to authorise surveillance powers like the acquisition of communications data and the use of 'Bulk Personal Datasets.'[98] These powers enable the gathering, retention and analysis of vast amounts of data which can then be used to, for example, cross check different data sets for 'commonalities in applications' in search of multiple benefit applications by one individual.[99] These surveillance powers are defined and analysed in Chapter 4 but suffice to show here how the digital evolution has enabled a shift away from cruder community surveillance efforts, like the system of 'overseers of the poor.' However, although subtler, these digital surveillance practices carry their own risks, such as discrimination, which is not always easy to identify or challenge given the discreet and clandestine manner in which data can now be analysed and processed.[100] There is a

[94] Poor Law Amendment Act 1834, s 27. Colquhoun famously distinguished between the 'deserving and 'undeserving' poor in: Patrick Colquhoun, *A treatise on the police of the Metropolis* (Mawman, 1800). Patrick Colquhoun, *A treatise on indigence* (Mawman, 1806). More discussion on Colquhoun in section 2.1 on 'Crime and disorder.'
[95] Higgs (n 70) 69.
[96] Stephen Walker, 'Expense, social and moral control. Accounting and the Administration of the Old Poor Law in England and Wales' (2004) 23 Journal of Accounting and Public Policy 85, 109.
[97] For example, in 2016 PM David Cameron confirmed that some 3,700 government inspectors are employed to investigate benefits fraud (thousands more than are deployed to investigate tax evasion by the rich), see HC Deb 13 April 2016, vol 68, col 347.
[98] Refer to Chapter 4 for definitions and analysis of these powers.
[99] Simon Atkinson, 'How can credit reference agencies catch benefit cheats?' *BBC News* (London, 10 August 2010).
[100] See Chapter 4, Part 2, section 1.2.3 for discussion on issues of discrimination posed by big data surveillance.

downside, therefore, to the more discreet practices of surveillance brought about by the evolution of the digital. These issues are considered further in subsequent chapters.

Although the techniques used under the Poor Laws were intrusive, severe and stigmatised the poor, detailed recording and community surveillance was an effective way of regulating the system and safeguarding against abuse. Today, technology enables more discreet monitoring of those in receipt of state benefits and benefit fraud can be detected without the need to publish a list of those receiving such support. Without these technologies, however, cruder techniques such as those listed above were arguably necessary to protect the state – which had, via the poor relief system, opened itself up as a resource for the economic wellbeing of both the individual and the local community.[101] Thus, whilst the surveillance used may have had a negative impact on the poor, it also protected the wider community and governmental interests. This supports the above argument that surveillance is never entirely 'good' or 'bad' but is also never neutral.

2.1.3 Summary

The above examination of surveillance in the context of taxation and social welfare has served to distinguish between information gathering and surveillance. The former is benign, does not collect information in excess of what is needed, and is considerably more transparent. The latter, on the other hand, is never entirely benign or malign and relies on information to identify and investigate an individual but not all of the information gathered will be of relevance or use. As noted above, the digitalisation of records has enabled more discreet surveillance practices to be used in the investigation of welfare recipients. However, as subsequent chapters will demonstrate, with this subtlety comes other risks, such as issues of transparency and discrimination. The extent to which the law has recognised and responded to these challenges presented by the digital surveillance landscape is considered in Chapter 4 and 5.

[101] Christopher Dandekar, Surveillance, Power and Modernity. Bureaucracy and Discipline from 1700 to the Present Day (Polity Press, 1990) 202-203.

2.2 Crime and disorder

Surveillance has a long history in the context of crime and social disorder. The roots of surveillance in this context are especially evident from the 17th to 19th centuries where the growth of capitalist global trade led to an expansion of urban living with 'outsiders' being attracted by higher wages, better food supplies, and more comprehensive poor relief.[102] 'Outsider' men and women were referred to as the 'master-less' and 'unshackled,'[103] and were accredited with giving birth to a 'many headed monster'[104] of social issues such as, begging, stealing, and prostitution which - coupled with a growing criminal underworld - exposed the 'obsolete nature of traditional mutual surveillance and security.'[105] Building on the previous discussion of more localised surveillance of the poor, this section traces the development of a more comprehensive, organised system of central surveillance from the 17th to 19th centuries.

2.2.1 Informal surveillance

As mentioned above, local communities were encouraged to watch over those in receipt of poor relief to ensure that they were 'deserving.' Whilst similar informal surveillance practices continued into the 18th and 19th centuries, they were structured more formally into societies which were largely formed by middle-class religious groups seeking to suppress deviance and immorality among the lower classes. For example, 'The Society for the Suppression of Vice' ('SSV') sought to police the morals of the lower classes on the premise that:

> 'The laws are good but they are eluded by the Lower Classes, and set at nought by the Higher. The laws are good: but they have fallen into

[102] Roy Coleman and Michael McCahill, *Surveillance and Crime* (Sage, 2011) 45.
[103] Vic Gatrell, 'Crime, Authority and the Policeman-State' in Francis Thompson (ed) *The Cambridge Social History of Britain 1750-1950, Volume 5: Social Agencies and Institutions* (Cambridge University Press, 1990) 254.
[104] John McMullan, 'Social Surveillance and the rise of the "police machine"' (1998) 2 Theoretical Criminology 93, 95.
[105] Zygmunt Bauman, *Legislators and Interpreters* (Cambridge Polity Press, 1987) 41.

> contempt, and require the zeal, the activity, the discretion as such a society as this to renovate their vigour.'[106]

Similarly, in line with Colquhoun's characterisation of the 'deserving and undeserving' poor, 'The Society for the Suppression of Mendacity' tested and scrutinised paupers to determine whether they were deserving of help, or a fraud deserving of punishment. These societies operated on a broad understanding of 'immorality,' including in its definition: drunkenness, cursing, gambling and other popular past-times. Whilst SSV and other societies had no legal authority to punish such 'immoral' behaviour, their work 'fed into calls for more bureaucratic and rationalised policing and surveillance concomitant with today's ideas of policing.'[107]

2.2.2 'Police intellectuals'

The condemnation of the lower classes as a breeding ground for criminal activity and immorality can also be seen in the theorisations of surveillance during the 18th and 19th centuries, namely in the work of 'police intellectuals:' John Fielding; Patrick Colquhoun; and, Jeremy Bentham.[108] These reformers positioned policing and surveillance as central to the investigation, inspection, and punishment of the idle, immoral poor and the criminal class. Each proposed a system that strove to create a system of centralised surveillance to prevent and deter criminal behaviour and which focussed on the lower classes who they deemed incapable of exercising self-restraint in their enjoyment of popular culture activities like drinking and gambling.[109]

Variances exist between each of the reformers' models but they agree on the importance of the codification and classification of criminals. For example, Fielding advocated the creation of a criminal register for tracking and investigating crimes.[110] Similarly, Colquhoun, writing in the 1790s into early 19th Century, called for the creation of a centralised police force responsible for recording crimes and criminals,

---

[106] Richard Watson Lord Bishop of Landaff (SSV representative), A sermon preached before the Society for the Suppression of Vice ('SSV') in the Parish Church of St George (3rd May 1804).
[107] Coleman and McCahill (n 102) 47.
[108] As referred to by McMullan (n 104) 107.
[109] Ibid.
[110] Coleman and McCahill (n 102) 48.

as well as a centrally-organised intelligence service and a network of private informants.[111] Colquhoun also placed the duty of policing the lower class on individuals who held a position of authority in society (such as teachers, clergy, and doctors) in order to help with the moral instruction of the poor.[112]

Bentham, who influenced Colquhoun, also viewed surveillance as key to preventing the immoral behaviours of the poor and reforming the criminal. As will be shown in Chapter 3, Bentham is perhaps most famous for his design of the 'prison-panopticon' in which he aimed to create such an omnipresent gaze over inmates that they eventually undertook self-surveillance and, ultimately, self-discipline.[113] Bentham thus sought to condition the mind of the criminal via surveillance rather than to punish his body through physical retribution. In line with Fielding and Colquhoun, the prison-panopticon also relied on a comprehensive system of record-keeping whereby any bad behaviour by an inmate was recorded by the guards and watchman.[114] This record-keeping was clearly surveillant in nature as it was 'in case of' any bad behaviour occurring instead of every morsel of information being used for a specific, more administrative purpose.

Whilst not all of the reformers' recommendations were adopted by government, they are reflective of elite thinking at the time. They are also considered to have played an important part in the development of the surveillance state by paving 'the way for that persistent surveillance which characterises modern policed society.'[115] This is further demonstrated in the following discussion of the development of a 'policeman-state' in the 19th century.

2.2.3 Birth of the 'policeman-state'

The following demonstrates that at least with regard to principles of classification, centralisation, prevention, and deterrence, the development of a 'policeman-state' (and

---

[111] Colquhoun, A treatise on the police of the Metropolis (n 94).
[112] Colquhoun, A treatise on indigence (n 94).
[113] Bentham (n 5).
[114] Ibid.
[115] John McMullan, 'The arresting eye: discourse, surveillance and disciplinary administration in early English police thinking' (1998) 7 Social and Legal Studies 97, 123.

the surveillance activities that burgeoned as a result) was informed by the ideals of the 'police intellectuals,' but by no means replicated the models proposed.

During the 1820s, there was increased elite anxiety over growing social disorder and crime. Gatrell questions how well-founded these anxieties were, suggesting that the problem of crime was actually exacerbated by the discourse around crime rather than being more problematic in itself, or at least to the extent felt by the upper classes.[116] Regardless, the Metropolitan Police was created in 1829 and a decade later the Rural Constabulary Act 1839 was passed which established the organisation of the first uniformed police force within and outwith London.

The 'new police' were directly responsible to the Home Secretary and thus represented an arm of the central state. They were provided with a broad legal remit, reporting on the lower classes enjoyment of recreational activities like gambling, drinking, dog-fighting and horse racing which - due to their supposed inability to exercise self-restraint – were considered to breed immorality, idleness and crime. In his analysis on the Liverpool City Police established in 1836, Coleman demonstrates the extent to which classification played a part in the work of the new police. For example, geographical areas of the lower classes were demarcated by police to facilitate the physical surveillance of property and streets where poorer people typically congregated.[117] The Metropolitan Police also published information on offenders, crime and its consequences in a 'Police Gazette' – which had been suggested by reformers Fielding and Colquhoun.[118]

Despite the above, the codification and record-keeping practices of the early uniformed police remained limited, with emphasis being placed on the deterrence of crime rather than the solving of crime. Whilst the police intellectuals clearly advocated a greater system of record-keeping than what materialised in the 19th century, their emphasis on prevention and the centralisation of police and surveillance is evident. More sophisticated record-keeping did eventually materialise towards the end of the

[116] Gatrell (n 103) 249.
[117] Coleman and McCahill (n 102) 63. See also Higgs (n 70) 93.
[118] Coleman and McCahill (n 102) 49; Higgs ibid.

19th century with, for example, a criminal registry being established under the Habitual Criminals Act in 1869. This was intended to distinguish the criminal population deserving of strict state surveillance from the law-abiding majority whose privacy had not been forfeited.[119] Photographs of criminals also came to be stored in the registry under the 1871 Prevention of Crimes Act and some local police forces maintained their own register of illustrations of criminals.[120]

2.2.4 Summary

Whilst the policing and surveillance system that developed did not achieve the same level of discipline and control desired by the 'societies against vice' or the 'police intellectuals,' it demonstrates an upward trajectory of state surveillance practices and - towards the end of the 19th century - a growing reliance on record-keeping for the tracking of offenders and investigation of crimes. It also demonstrates the impact of discourse on the use of surveillance. For example, the discourse around crime and social disorder led to surveillance being strongly focussed on the lower classes – a clear response to elite anxieties over the 'great unwashed.' This demonstrates the ability of some groups to co-ordinate and shape surveillance regimens whilst others bear the brunt of its impact.

The issues and debates surrounding surveillance in the 19th century continue to be seen today, although as will be shown in Chapter 3, democratisation of (surveillance) technology has granted the individual some power to return the gaze of the watcher meaning that she is not as powerless or passive as the subjects of the panopticon. Chapter 4's illustration of the IP Act's response to the contemporary surveillance landscape also demonstrates a widening of the gaze to incorporate non-suspects with the introduction of bulk powers aimed at everyone as opposed to just targeted individuals and groups. Although, as will also be shown, the breadth of these powers does not eliminate the risks of discrimination and bias which continue to be expressed in the application of surveillance. Finally, the surveillance trends of the 18th and 19th centuries show that the pre-emptive and preventive approach to crime is no new

[119] Higgs (n 70) 95.
[120] Ibid 96.

phenomenon, but rather, one that has developed over time.[121] Surveillance as a tool for the prevention of crime further supports the definition of surveillance set out above – that it involves an element of 'in case of' with subjects being watched 'in case of' wrongdoing as opposed to every morsel of information gathered being used for a specific purpose.

2.3 War

This section examines the use of surveillance during times of war - a context within which rights and freedoms are legally accepted as secondary to the life of the nation.[122] This section will thus provide a comparison to earlier sections which focussed on the use of surveillance during peacetime for the purposes of maintaining order, control, and discipline within the state. Focus is placed on the 20th century where there was an intensification of war, information gathering, and surveillance.

2.3.1 Information gathering during and post-WWI (1914-1918)

With the threat of WWI hanging overhead in early 20th century Britain, information gathering became increasingly important for achieving military preparedness. In 1915, the National Registration Act was passed requiring men and women between the ages of 15 and 65 to be registered with the armed forces and supplied with a certificate by the General Registry Office ('GRO') which was to be carried at all times. This certificate functioned as 'an identity card in all but name.'[123] The resulting availability of individuals' information also led to other duties being undertaken by the GRO, such as the administration of ration books and the supply of information on enemy aliens living in the UK to MI5.[124] The benefits of the registration system under the 1915 Act

[121] As noted by Coleman and McCahill (n 102) 75.
[122] For example, Article 15 ECHR allows for derogation in times of emergency, affording governments the possibility of derogating in a temporary, limited and supervised manner from their obligation to secure certain rights. For application of Art 15 see, *Lawless v Ireland (no 3) (1979-80)* 1 ECHR 15; *Aksoy v Turkey* (1997) 23 ECHR 553; *Ireland v UK* (1979-80) 2 ECHR 25.
[123] Higgs (n 70) 137.
[124] General Register Office, *77th Annual Report of the Register General for 1914* (London: HMSO, 1916) viii.

subsequently led to the creation of the Hayes Fisher Committee in 1917 which was established to consider the continuance of the system post-WWI.[125]

Whilst the aim of the committee was to highlight the value of state information gathering in the enforcement of both rights and obligations of the individual, proposals to permanently establish the national register were met with significant public opposition.[126] The Hayes Fisher Committee Report illustrated many administrative benefits of the system, including: the improvement of registration of births and deaths, the enforcement of school attendance, and medical benefits.[127] However, a public fear of 'prussianism', which referred to over-interference by the state, proved to be a major obstacle to the establishment of a national register during peacetime - where the context of war no longer served to justify the same level of state involvement in the lives of its citizens.[128] The change of context thus served to alter the nature of the national registration system from one of benign information gathering to one of surveillance. The scheme was subsequently abandoned in the 1920s.

National registration was not the only wartime measure that the government sought to establish in post-war Britain. The Ministry of National Service also suggested that all ex-soldiers be fingerprinted for the prevention of fraud in the payment of war pensions.[129] As per the definition of surveillance above, this system of fingerprinting would go beyond benign information gathering as its purpose was to prevent *potential* fraud by ex-soldiers. However, fearful of causing offence to ex-servicemen in the eyes of the British public (by implying that they would commit such a crime), this proposal was also deemed inappropriate and was shelved alongside the continuance of the national register.[130] Storing the fingerprints would have been an exercise of

---

[125] Higgs (n 70) 137.
[126] Ibid 138.
[127] Departmental Committee on National Registration, Report of the Sub-Committee Appointed to Consider a System of General Election (PRO RG 28/4, 1918).
[128] See, HL Deb 5 July 1915, vol 73, col 135; HL Deb 25 January 1916, vol 20, col 997. See also, Jon Agar, 'Modern Horrors: British Identity and Identity Cards' in Jane Caplan and John Torpey (eds) *Documenting Individual Identity: The Development of State Practices in the Modern World* (Princeton University Press, 2001).
[129] Higgs (n 70) 139.
[130] Ibid.

surveillance as doing so would have been 'in case of' a crime (fraud) occurring. Whilst this surveillance could have provided valuable financial protection to ex-soldiers, the potential damage to public opinion proved more important. This supports the argument that surveillance is never entirely benign nor malign, but is also never neutral.

The above examples demonstrate the acceptance of greater state involvement in private lives within the context of war, but also show the push-back against these same practices during peacetime – where the threat of war no longer worked to justify the same level of interference with the privacy of its citizens. Demonstrated here, therefore, are the peaks and troughs of information gathering during wartime and peacetime. However, the same cannot be said for the covert surveillance practices developed during the World Wars which failed to be clawed back upon the cease fire in quite the same way.

2.3.2 Surveillance during and after the World Wars

In 1909 the 'Secret Service Bureau' (which later became MI5 and MI6) was established to gather intelligence on German espionage activity in Britain. The Bureau was established in response to recommendations of a sub-committee of the Committee of Imperial Defence investigating 'the nature and extent of foreign espionage that is at present taking place within this country and the danger to which it may expose us.'[131]

Based on the intelligence gathered by the Bureau, Germans and communists were prosecuted under the Defence of the Realm Act 1914 – despite a serious lack of legal regulations on the surveillance practices used by the intelligence agencies. Whilst laws covering some surveillance powers existed, such as The Telegraph Act 1868 governing the interception of telegraph communications, they were limited and failed to cope with technological advances in signal and communications surveillance following WWII. The lack of surveillance law at this time was capitalised on by government who 'developed a pattern of using the law – or its lack of coverage – to

[131] The sub-committee was led by Robert Haldane, Secretary of State for War in Asquith's liberal government. See, Jeffrey Richelson, *A century of spies: intelligence in the Twentieth century* (Oxford University Press, 1995); Christopher Andrew, *The Defence of the Realm: the authorised history of MI5* (Penguin, 2010).

extend surveillance.'[132] For example, in 1911 Home Secretary Winston Churchill granted general warrants for postal interception, rather than specific warrants, in order to intercept all the mail of an individual or group of persons.[133] Importantly, such general surveillance powers were not only used in the context of war, but also against political activist groups like the suffragettes.[134] Similarly, with regard to telephony interception, no law criminalising the tapping of telephone communications existed until the passing of the Interception of Communications Act in 1985.[135] This type of interception was undertaken without a warrant until review of the policy by the Home Secretary and Post-master General in 1937.[136]

Although developed in anticipation of war, the lack of corresponding legal regulation enabled surveillance practices to seep outwith the context of war. Telegraph, postal, and telephony surveillance continued into the post-war context, eventually being used for internal communications once external threats from Germany and Russia receded. Despite increasing use of these techniques, it was not until the 1990s when more formal and comprehensive laws were passed (namely the Police Act 1997 and the Regulation of Investigatory Powers Act 1997 ('RIPA')), that surveillance was brought within the reach of the law. Although as shown in Chapter 2, these laws were still insufficient.

2.3.3 Summary

From the above, it can be seen that the greater transparency with which the information gathering system operated during WWI facilitated subsequent debate on the legitimacy of extending practices into the post-war period. The surveillance system, on the other hand, which lacked any meaningful and formal legal regulation, was able to expand into the post-war context with political actors like Winston Churchill capitalising on

---

[132] Simon McKay and Jon Moran, 'Surveillance powers and the generation of intelligence' in Genevieve Lennon and Clive Walker (eds), *Routledge Handbook of Law and Terrorism* (Routledge, 2015) 137.
[133] Ibid.
[134] David Stafford, *Churchill and the secret service* (Abacus, 2001) 44-45.
[135] Laurence Lustgarten and Ian Leigh, *In from the cold: national security and parliamentary democracy* (Clarendon Press, 1994) 324-327.
[136] Home Secretary, Interception of communications in the United Kingdom: a consultation paper (Cm 4368, 1999) para 2.1.

the law's silence. As shown in subsequent chapters, reduced opportunities for transparency caused by a lack of regulation is also seen in the 21st century with various instances of surveillance powers being used without adequate legal regulation. Snowden made this particularly evident in his exposure of long-term mass surveillance practices used in the UK and US without the necessary basis in law. The above sections also underline the importance of the scope and application of surveillance powers. For example, in section 2.3.1 it was shown that national registration, certificates, and fingerprinting were accepted as necessary for the defence of the realm during wartime. However, during peacetime when these powers became aimed at the 'in-group' – the general population and demobilised soldiers – they were no longer justified. This contrasts with the acceptance of surveillance powers covered in section 2.3.2 which were aimed at 'aliens' and citizens undermining the state. This is perhaps why such outrage ensued following the Snowden disclosures as the whistleblower revealed that surveillance was now being aimed at the 'in-group' instead of just the 'alien' or 'outsider.'

2.4 National security

'National security' is a notoriously difficult concept to define and has arguably become even more so with the blurring of lines between crime, war, and terrorism. For example, the UK's 'National Security Strategy,' considers 'national security' to include: organised crime; environmental accidents; global health risks; energy security; and economic uncertainty - in addition to more traditional threats emanating from terrorism, nuclear warfare, and espionage.[137] Furthermore,

> '[t]he transforming capabilities of ICTs make it increasingly difficult to distinguish between warfare, terrorism and criminal activities' as an extremist political group might carry out all three.[138]

[137] Home Office, The national security strategy and strategic defence and security review 2015: a secure and prosperous United Kingdom (Cm 9161, 2015) Chapter 2.
[138] Douglas Thomas and Brian Loader, Cybercrime: law enforcement, security, and surveillance in the Information Age (Routledge, 2000) 3.

In response to this expansion of the national security context, surveillance has intensified; expanding in scope to incorporate more individuals and identify more threats to national security.[139] This is demonstrated in Chapter 4's analysis of the bulk surveillance powers introduced under the IP Act.

Discussion on the role of surveillance in the national security context is thus broad and varied. Therefore, this section narrows the discussion of surveillance within the national security context by examining its use: (i) in the Elizabethan era (1158-1603) and, (ii) during the Troubles in Northern Ireland (1968-1998).[140] These periods have been selected on the basis that they demonstrate the evolution of surveillance in response to different types of national security threats. They also reveal points at which surveillance has been deemed as excessive, whether legally, socially, or politically and, therefore, rejected. This discussion therefore provides a useful point of reference for subsequent analysis of surveillance powers used in the current national security context in Chapter 4.

2.4.1 Espionage under Elizabeth I (1558-1603)

As the last Tudor of direct lineage Elizabeth relied heavily on espionage for the protection of her life.[141] Upon succession to the throne, Elizabeth faced the religious question of what form the Church of England would take.[142] With the political advantages of a Protestant settlement in mind, the Queen's decision was finalised with the re-establishment of the Church of England's independence from Rome under the Act of Supremacy 1558 and the confirmation of the form it should take under the Act of Uniformity 1559.[143] Despite Elizabeth initially taking a moderate approach towards Catholics, some of her actions raised their suspicions of her.[144] Elizabeth's suspicion

---

[139] Clive Walker, 'Championing local surveillance in counter-terrorism' in Fergal Davis, Nicola McGarrity, George Williams (eds.) *Surveillance, counter-terrorism and comparative constitutionalism* (Taylor & Francis, 2014), 23; Kirstie Bell and Frank Webster, *The intensification of surveillance: crime, terrorism and warfare in the information age* (Pluto Press, 2003).
[140] Walker ibid 23.
[141] Alan Haynes, *The Elizabethan Secret Service* (Kindle DX Version, The History Press, 2009) vi.
[142] Wallace McCaffrey, *Elizabeth I* (Edward Arnold, 2001) 48.
[143] Ibid 51.
[144] For example, Elizabeth disregarded Catholic ancient nobility and gentry by restricting their power and replacing them with 'new men' in matters of civil administration, see Christopher Haigh, *Elizabeth I* (Routledge, 2013) 182. Elizabeth's decision to keep Mary Queen of Scots hostage also

of Catholics was also raised by the issuance of a Papal Bull in 1570 excommunicating and deposing her.[145] Hitherto, she had adopted a fairly lenient approach towards Catholics in the hope that Catholicism would recede.[146] However, as Catholic activism grew so too did the threat to the Queen's reign, eventually leading to Catholics being treated as enemies of the state and the practice of Catholicism becoming punishable by law in 1571.[147]

To help enforce these laws and uncover plots against her life, Elizabeth adopted espionage practices from Renaissance Italy. The work of her spymasters revealed the true extent of Catholic resentment, exposing numerous plots and rebellions against her life.[148] The development of a comprehensive spy network and the role of informants thus proved integral to the suppression of Catholic rebellion, the protection of Elizabeth and, therefore, national security. Whilst the aggressive surveillance of Catholics successfully suppressed revolt and thwarted plots against Elizabeth's life, it did not eliminate the Catholic threat with attempts being made against the Queen's life until her (natural) death in 1603.[149] Her surveillance regime did, however, serve to enforce the obedience of most of her subjects (both Catholic and Protestant) who under the watchful eyes of the spymasters and informants, were disciplined into conformity.[150] The success of Elizabeth's espionage practices contributed to the perpetuation of surveillance across the UK, which Elizabeth took great pride in.[151] Indeed, the attraction of being able to suppress rebellion, coerce loyalty, and demand

---

sparked resentment as it extinguished Catholic hopes of a union between Mary and the Duke of Norfolk, see, Diana Newton, *North-East England, 1569-1625: Governance, Culture and Identity* (Boydell Press, 2006), 122. See also Richard Reid, 'The Rebellion of the Earls, 1569: The Alexander Prize 1905' (1906) 20 Transactions of the Royal Historical Society 171, 177.

[145] Haigh ibid 51.

[146] Ibid. Repression also posed administrative difficulties.

[147] Statutes of the Realm 1571 (13 Eliz. 1), s.2.

[148] For example, the Babington plot to overthrow Elizabeth was discovered upon the interception of correspondence between Mary Queen of Scots and fellow conspirator, Anthony Babington, see Haigh (n 141) 149. The Ridolfi and Throckmorton plots were also exposed and thwarted by the Queen's spymasters, see Haynes (n 138) xiv.

[149] McCaffrey (n 142) 354. Although, exact cause of death is debated.

[150] Ibid.

[151] Haynes (n 141) xii.

the acceptance of state power as legitimate has proved irresistible for future monarchs and governments - arguably making surveillance one of Elizabeth I's greatest legacies.

However, the suppression of dissension throughout Elizabeth's reign does not only demonstrate the value of surveillance for national security, but also its capacity to oppress individuals and entire communities, in this case, Catholics. The system of surveillance under Elizabeth I functioned by suppressing the religious freedom of individuals and, in turn, threatened the very identity of their sense of self. Elizabeth's surveillance may thus be seen as reducing her subjects to 'docile bodies' amenable to direction and control. Indeed, this is what makes surveillance such an effective tool for enforcement as it not only enables the identification of dissenters, but also induces within individuals such a degree of (self-)discipline that their obedience is procured.

In summary, it would be incorrect to label the system of surveillance under Elizabeth I as 'bad' as it was fundamental to the protection of the throne and national security. It was also somewhat justified by the attacks made on Elizabeth's life throughout her reign. However, it is equally unfounded to view the surveillance under Elizabeth I as 'good' as it oppressed the religious freedom of individuals and disenfranchised the Catholic community – the majority of which were undeserving of such suspicion or treatment. The above discussion thus supports Lyon's argument that surveillance is neither good nor bad, but is also never neutral.

Whilst there are times that rights can be lawfully infringed for the purposes of securing national security, it is a delicate balance that must be struck between the protection of the state and justifiably interfering with an individual's rights. The infringement of a right does not signify unlawful surveillance as exceptions and derogations are permitted for the very reason that some circumstances demand the implementation of more aggressive methods of state action to safeguard national security. However, it is when such methods are employed to the extent that they become disproportionate to that aim that questions over their lawfulness arise. Characteristics of such disproportionate surveillance are identified in Chapter 2's analysis of the ECtHR's Article 8 surveillance case law, enabling the UK surveillance legal landscape to be assessed accordingly in Chapter 4.

2.4.2 Surveillance in counterterrorism

First, it is necessary to conceptualise terrorism – or at least summarise attempts to conceptualise terrorism. To date, there is no customary international crime of terrorism and concepts of terrorism under national laws vary significantly.[152] Defining terrorism is thus difficult and contentious, particularly with regard to whether political violence is ever justified.[153] However, at the international level there is broad consensus that terrorism includes 'criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes.'[154]

The law treats terrorism separately from ordinary crime due to particular characteristics requiring a different approach by government and law enforcement. A major difference is the global nature of terrorism which has become particularly pronounced in the post-9/11 climate. For example, attacks have been carried out across the globe by terrorist groups like ISIS in: London; Madrid; Paris; Boston; Brussels; Manchester, and; Barcelona.[155] Furthermore, unlike ordinary crime, terrorism threatens the state as well as individuals, being commonly perceived as 'an assault on the foundations of liberal, constitutional systems.'[156] Consequently, terrorism is treated as an exceptional criminal phenomenon deserving of exceptional measures extending beyond the traditional boundaries of criminal law, and that treats terrorists as enemies of the state as opposed to just citizens who have acted criminally.[157]

In terms of where surveillance fits within the counterterrorism context, it has always played a crucial role in the protection of the state (as demonstrated in the previous

---

[152] UNCHR, 'Report of the special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism' (28 December 2005) E/CN.4/2006/98, 2005, Part 3. See also, Ben Saul, 'Terrorism as a legal concept' in Lennon and Walker (n 132) 19.
[153] Saul ibid.
[154] Core elements of terrorism agreed in UNGA 'The Declaration on Measures to Eliminate International Terrorism, in the annex to UN General Assembly Resolution' (9 December 1994) A/RES/49/60.
[155] Mariona Llobet-Angli and Aniceto Masferrer, 'Counter-terrorism, emergency, and national laws' in Lennon and Walker (n 132) 38.
[156] Ibid 39.
[157] Ibid.

section).[158] As argued in Chapter 4, the transferral of life online by the 'bad' as well as the 'good' has led to the significant extension of surveillance powers in the UK to prevent and combat terrorism. In order to subsequently highlight the intensification of surveillance in the UK within the counterterrorism context, this section examines the role of surveillance during 'the Troubles' in Northern Ireland. This will provide a benchmark to Chapter 3's analysis of surveillance used in the current counterterrorism context. This previous era of terrorism lacked the same technological advantages enjoyed by present-day terrorist groups who are now able to network, plan, and co-ordinate attacks from different locations across the globe via the internet. This will enable subsequent analysis of UK surveillance laws which have sought to respond to the digitalisation of society, or in this case, the digitalisation of terrorism.

2.4.2.1 Surveillance in Northern Ireland during the Troubles (1968-1998)

The Metropolitan Police Special Branch ('MPSB') was established in 1883 during the Fenian 'Dynamite Wars' in London and led the way for intelligence-led policing against Irish Republican terrorism in the UK.[159] However, in Northern Ireland the Special Branch of the Royal Ulster Constabulary (RUC Special Branch) took the lead with UK intelligence services typically only playing a supporting role to the RUC Special Branch in Northern Ireland.[160]

In 1969 violence on the streets of Derry/Londonderry marked a resurgence of Irish Republican Army ('IRA') terrorism in Northern Ireland and the dawn of the Troubles.[161] The unrest grew to overwhelm the resources of the RUC, forcing the British Army to intervene in Northern Ireland.[162] With RUC intelligence severely lacking, the Army set to filling in the intelligence gaps via the use of overt and covert

---

[158] David Anderson QC describes 'investigatory powers' as playing a 'vital part' in the fight against terrorism, in Independent Reviewer of Terrorism Legislation, *A question of trust* (Crown, 2015) para 1.16.
[159] Lindsay Clutterbuck, 'Countering Irish republican terrorism in Britain: its origin as a police function' (2006) 18 Terrorism and Political Violence 95; Ray Wilson and Ian Adam, *Special Branch a history 1883-2006* (Biteback publishing, 2015).
[160] Clutterbuck ibid.
[161] Laura Donohue, Counter-Terrorist Law: And Emergency Powers in the United Kingdom 1922-2000 (Irish Academic Press, 2001) 117.
[162] The RT Hon The Lord Saville of Newdigate, The Hon William Hoyt OC, The Hon John Toohey AC, *Report of the Bloody Sunday Inquiry* (HC 2010-2011, 29-1) para 7.738.

surveillance measures.[163] The British Army subsequently engaged in observation practices and patrols coupled with the use of 'plain clothes'[164] units to surveil 'no-go' areas.[165] Much of the surveillance in Northern Ireland at this time was not technology based and was carried out by informants, also known as 'human intelligence' ('HUMINT').[166] The mass interception of communications between the UK and Ireland also took place between the years of 1990 and 1997 under the Interception of Communications Act 1985.[167]

HUMINT grew in importance following the failure of the British government's militaristic approach to IRA terrorism.[168] Whilst the informant system in Northern Ireland was considered valuable in quelling the chaos, criticisms burgeoned following the peace process in 1998.[169] Concerns arose over the questionable quality of the information gathered by informants, the threat posed to their life, and the ethical basis of the system.[170] There was also no statutory basis for the use of informants during the Troubles. Whilst case law and legal opinion provided some guidelines as to what was and was not acceptable for informants to do, 'The Report of the Patrick Finucane Review' (the 'de Silva' report') concluded that

---

[163] Ministry of Defence, *Land Operations Volume III – Counter-Revolutionary Operations* A/26/GS Trg Publications/3011 (Ministry of Defence, 1969), para 128.
[164] Bradley Bamford, 'The Role and Effectiveness of Intelligence in Northern Ireland' (2006) 20 Intelligence and National Security 4, 587.
[165] Report of the Bloody Sunday Inquiry (n 162) para 2.6.
[166] Clutterbuck (n 159) 101.
[167] This is examined in more depth in Chapter 2, section 2.1.4.1 which discusses the case of *Liberty and others v UK* (2009) 48 ECHR 1 where the ECtHR held that the interception regime under IOCA 1985 lacked sufficient safeguards and was thus unlawful under Article 8 ECHR.
[168] For example, significant unrest was caused by the killing of 13 civilians by British troops on 'Bloody Sunday' and over the use of give interrogation techniques which were later declared unlawful under Article 3 of the ECHR in *Ireland v UK* (n 122).
[169] Jon Moran, 'Evaluating special branch and the use of informant intelligence in Northern Ireland' (2010) 25 Intelligence and National Security 1, 2.
[170] For example, with it being alleged that informants carry out murder. See Clive Walker, 'Championing local surveillance in counter-terrorism,' in Lennon and Walker (n 132) 27. Although, Jon Moran argues that some of these criticisms have been overstated in Moran (n 169) 2.

> '[w]hilst certain parameters and guidelines could be extrapolated from case law and legal texts, it was both insufficiently clear and insufficiently comprehensive to provide detailed guidance for either an agent or an agent-handler.'[171]

In light of the serious offences undertaken by some informants during the Troubles, RIPA was passed to regulate the use and conduct of covert human intelligence sources ('CHIS'), requiring their use to be necessary, proportionate and compatible with human rights.[172]

Despite the above risks and issues with the use of informants during this period, they were not wholly unsuccessful in interrupting terrorist activity; fostering mistrust within terrorist groups and pre-occupying them with 'snuffing out' informers.[173] However, the sentiments of betrayal and mistrust were not only felt within the IRA but also across the wider Catholic community, especially with regard to the dispensing of justice.[174] In this sense, the surveillance during the Troubles may be seen as fuelling an already incredibly hostile civil conflict, as under Elizabeth I.

Aside from the top-down practices of surveillance, there was also considerable community surveillance during the Troubles.[175] Out of fear for one's own security, individuals watched over each other carefully, especially 'outsiders' not belonging to their neighbourhood. The closeness of Northern Irish communities provided a hotbed for communal surveillance, supporting the 'mechanisms of watching, surveillance and reaction to potential threats by others.'[176] Such communal surveillance thus reflects what Lyon calls, the two faces of surveillance – care and control.[177] Care because the

---

[171] The Rt Hon Sir Desmond de Silva QC, *The report of the Patrick Finucane Review* (HC 2012, 802-I) para 4.14 ('de Silva Report').
[172] RIPA 2000, Part II.
[173] Keith Maguire, 'The Intelligence War in Northern Ireland' (1988) 4 International Journal of Intelligence and Counterintelligence 2, 154.
[174] Steven Greer, 'The Supergrass system' in Paul Wilkinson and A M Stewart (eds) *Contemporary Research on Terrorism* (Aberdeen University press, 1987) 531. The usefulness of informants was also confirmed in the de Silva Report (n 171) paras 4.3-4.4.
[175] Nils Zurawski, '"I know where you live!" – aspects of watching, surveillance and social control in a conflict zone (Northern Ireland)' (2005) 2 Surveillance & Society 498.
[176] Ibid 504.
[177] David Lyon, *Surveillance society: monitoring everyday life* (Open University Press, 2001) 3.

community is protecting its members through surveillance, and control because the same community will punish deviations posing a threat to its security.[178] This supports his description of surveillance as a practice that is never either benign, malign, or neutral.

Surveillance during the Troubles was thus multi-layered, being carried out by police and intelligence agencies as well as individuals and communities. The culture of conflict may thus be seen as inducing a culture of surveillance that permeated the depths of Northern Irish society with everyone watching 'in case of' a threat to their security or neighbourhood materialising. The system of informants together with communal surveillance became integral to counterinsurgency efforts and, in turn, to the security of the state and the community. However, this culture of surveillance also bred a culture of suspicion with watching being extended from the enemy to one's own community. This arguably enhanced the antagonistic effect of the Catholic-Protestant divide with members of the same community looking upon each other suspiciously.

Chapter 3 shows that communal and interpersonal surveillance continues as a prominent feature in the contemporary surveillance landscape. In fact, it is shown to have been enhanced by the availability of (surveillance) technologies to individuals. However, in addition to its use in counterterrorism and crime settings, surveillance between individuals is now also used outwith these contexts as a means of developing and maintaining relationships. This is demonstrated via an analysis of social media and smartphones in Chapter 3 which shows that interpersonal surveillance has continued into the digital age but is now happening on different platforms and to a totally different scale. For example, 'hacktivists' who use computers to promote political ends, could be viewed as attempting to protect their neighbourhood but that neighbourhood is democratic society at large.[179]

---

[178] Zurawski (n 175) 506.

[179] 'Anonymous' and 'Lulz Security' are two widely known 'hacktivist' groups. The latter has carried out various political hacks including on the Federal Bureau of Investigation in the US, the US Senate and the Central Intelligence Agency websites. In 2013, 'Anonymous Africa' hacked 50 websites during the Zimbabwean election including those related to the ruling political party ('Zanu PF'). For more information see, Dai Davis, 'Hacktivism: good or evil' (*ComputerWeekly*, March 2014) <https://www.computerweekly.com/opinion/Hacktivism-Good-or-Evil> accessed 2 August 2018.

Surveillance in counterterrorism is further examined in Chapter 3 which demonstrates the extent to which contemporary surveillance practices, such as those exposed by Edward Snowden, rely on national security for their justification.[180]

3 Conclusion

This chapter has provided historical context, illustrating the various uses and consequences of surveillance across eras. Whilst surveillance trends and debates have evolved in the digital age, establishing their roots in British surveillance history enables subsequent developments brought about by the digitalisation of society to be identified. In turn, the IP Act's response to these developments can be critically assessed. This chapter has therefore provided a benchmark for subsequent discussion, enabling the impact of the digital evolution on the surveillance landscape to be subsequently illustrated.

This chapter has also served a definitional purpose by distinguishing surveillance as a practice related to, but separate from, information gathering – with surveillance beginning at the point from which information is gathered 'in case of,' as opposed to being absolutely necessary for achieving a stated aim or purpose. Chapter 2 demonstrates that this defining feature of surveillance creates greater scope for necessity and proportionality issues to arise under human rights law. Surveillance was also distinguished from information gathering practices by showing that it is never entirely benign or malign, but is also never neutral.

Finally, this chapter has shown that the legal regulation of surveillance in the UK has been slow to develop, leaving significant gaps in its protection of privacy and against arbitrariness and abuse. This was particularly evident upon examination of the surveillance practices used during and after the World Wars with interception lacking any legal mandate until well after its advent. Similarly, the use of informants in Northern Ireland lacked any legal basis which led to significant abuses and offences being carried out. Edward Snowden revealed that this legislative lag has persisted into

[180] Chapter 3, Part 2, section 2.3.

the 21st century with governments capitalising on gaps in the law to carry out the mass surveillance of communications.[181]

[181] As shown in Chapters 3 and 4.

Chapter 2 Defining privacy under the ECHR

Introduction

This thesis explores the definition of privacy under Article 8 of the ECHR via an examination of its application by the ECtHR, focusing on its surveillance jurisprudence. It is necessary to define privacy as it is on this basis that the impact of the IP Act's approach to the contemporary surveillance landscape is subsequently assessed in Chapter 5. This chapter thus serves a definitional purpose.

Although this thesis focusses on the suitability of UK surveillance law, some consideration is also given to the suitability of the ECtHR's application of Article 8 ECHR in the digital age. This is achieved by reference to the CJEU's approach to privacy in its recent surveillance case law, particularly how its determination of discretion offers potentially greater protection to privacy in the digital age. Consideration is also given to the scope for a group privacy right to be enjoyed under Article 8 which, as shown in Chapter 3, is becoming increasingly important in the age of 'Big Data' where vast amounts of personal data are gathered and processed without a pre-established goal. This makes it incredibly difficult to establish the type of individualistic, personal harm upon which Article 8 claims are typically based.

This chapter first analyses the ECtHR's application of Article 8 in its surveillance case law. This is structured under three main headings that mirror the structure of the ECtHR's assessment of interferences with this right: (i) engaging Article 8(1); (ii) the legality of interferences; and, (iii) justified interferences. This structure has been adopted for the purposes of clarity. Second, it is considered whether there exists any scope for groups to engage Article 8. This is relevant to subsequent discussion on the legal implications of the contemporary surveillance landscape where harm often occurs at a group or societal level as opposed to just on a personal or individual level. From this analysis, the ECtHR's concept of harm, victimhood, and expectations of privacy can be identified and examined in terms of whether they are reflective of the contemporary surveillance landscape illustrated in Chapter 3. This will enable conclusions to be drawn as to the relevancy of the ECtHR's approach within the

current surveillance climate. The chapter concludes with a summary of the scope of Article 8, underlining the most relevant aspects of the ECtHR's definition of privacy which will then be used to critically assess the IP Act's approach to aspects of the contemporary surveillance landscape in Chapter 5.

1 Engaging Article 8(1)

Article 8(1) states: 'everyone has the right to respect for his private and family life, his home and his correspondence.' As mentioned in the introduction to this thesis, the ECtHR adopts a pluralistic approach to the definition of 'private life,' defining it as a 'broad term not susceptible to exhaustive definition.'[182] Consequently, the concept of a 'private life' can be difficult to understand and apply, particularly for domestic courts.[183] However, it also provides a capacious platform for complaints that would, perhaps, otherwise fail to engage the ECHR.[184] Whilst the ECtHR has abstained from offering an all-encompassing definition of 'private life,' it has confirmed that certain circumstances do fall within its scope, including: the 'right to establish and develop relationships;'[185] the right to 'pursue the development and fulfilment of the personality;'[186] 'a right of access to data,'[187] and the 'zone[s] of interaction of a person with others, even in public.'[188] In line with privacy scholars like Westin, Rossler, Solove, and Rosen,[189] these aspects of private life have led the ECtHR to consider the more general 'notion of personal autonomy as an important principle underlying the interpretation of its [Article 8's] guarantees.'[190] As demonstrated below, the open-endedness of 'private life,' together with the other components of Article 8(1) (the

[182] Niemetz v Germany (n 23); Peck v UK (n 23); Pretty v UK (n 23).
[183] See Nicole Moreham, 'The right to respect for private life in the European Convention on Human Rights: a re-examination' (2008) 1 European Human Rights Law Review 44, 44. See Introduction, section 2.3.
[184] Article 8 has been used as a platform for a number of complaints, such as: the protection of one's living environment from pollution (See, *Kyrtatos v Greece* (2005) 40 ECHR 16; the living conditions of gypsy travelers (*Chapman v UK* (2001) 33 ECHR 18; issues related to euthanasia (*Pretty v UK*, n 23); abortion rights (*A, B, and C v Ireland* (2011) 53 ECHR 13); and, gender recognition for transsexuals (*Goodwin v UK* (2002) 35 ECHR 18).
[185] See, for example, *Friedl v Austria* (1996) 21 ECHR 83, para 44.
[186] *Burghartz v Switzerland* (1994) 18 ECHR 105, para 47.
[187] *Gaskin v UK* (1990) 12 ECHR 36, para 37.
[188] *PG and JH v UK* (2008) 46 ECHR 51, paras 56-57.
[189] See section 3.2 of Introduction.
[190] *Pretty v UK* (n 23) para 60.

protection of family life, home and correspondence), have provided a broad platform for various complaints against surveillance regimes and practices to be heard.

Under the themes of gathering, processing, and retention, this section identifies the stages at which different surveillance practices are capable of engaging Article 8(1). It is necessary to establish the points at which Article 8 is engaged in order to subsequently assess the coverage of the IP Act in Chapter 4. For example, where the IP Act fails to recognise and regulate surveillance deemed capable of interfering with Article 8 by the ECtHR, there is clearly a deficiency in its coverage of the contemporary surveillance landscape that poses a risk to privacy.

1.1 Gathering

'Gathering' refers to the initial stage of surveillance and can be carried out either 'covertly' or 'overtly.'[191] RIPA defines surveillance as 'covert:' 'if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.'[192] Covert surveillance is either: 'directed' – aimed at a specific target as part of an operation – or, 'intrusive' - carried out in relation to anything taking place on any residential premises or private vehicle, and involving the presence of an individual on the premises or in the car, or is carried out by using a surveillance device (eg bugging a house or car).[193] No definition of overt surveillance is provided under UK surveillance law but its meaning can be inferred from RIPA's definition of covert surveillance as: (i) not directed (ie not aimed at a specific target); (ii) non-intrusive (no devices are used on private property to covertly listen to or monitor an individual or group); and, (iii) measures are not taken to ensure that individuals remain unaware of its presence (eg CCTV).

This section is only concerned with gathering practices that are singularly capable of triggering Article 8(1) as opposed to when used in conjunction with another practice, such as the processing or retention of material which are discussed in sections 1.2 and

[191] See Chapter 1 for discussion on distinction between information gathering and surveillance.
[192] RIPA, s 26(9)(a).
[193] RIPA, ss 26(2) and 26(3).

1.3, below. Thus, this section deals only with interception as other types of surveillance fail to engage Article 8 automatically.

1.1.1 Interception

The ECtHR has consistently held that the interception of communications automatically engages an individual's right to private life and correspondence, regardless of whether or not the information was subsequently processed or stored.[194] This is seen in *Malone v UK* where the applicant, an antiques dealer suspected of dealing in stolen goods, claimed that his telephone calls had been wire-tapped.[195] Noting that telephone conversations are covered by the notions of 'private life' and 'correspondence' the ECtHR held that the measure constituted an interference by a public authority with Article 8.[196]

The ECtHR has subsequently held that the interception of other methods of communication (eg emails)[197] can engage an individual's Article 8 right, thus demonstrating an awareness of technological change within the sphere of communications.[198]

1.1.2 Klass: an expansion of victimhood

The 'mere existence' of legislation permitting interception is also capable of engaging Article 8(1).[199] In principle, Article 34 of the ECHR prohibits non-victims from challenging *in abstracto.*[200] However, in *Klass v Germany* the ECtHR justified a deviation from this Article by underlining the difficulties arising from the inherently secret nature of surveillance rendering it near impossible for an individual to 'point to any concrete measure specifically affecting him.'[201] This was especially the case where individuals are not 'subsequently informed of the measures taken against them'

---

[194] See *Kopp v Switzerland* (1999) 27 ECHR 91, para 53.
[195] *Malone v UK* (1985) 7 ECHR 14.
[196] Ibid, para 64.
[197] *Halford v UK* (1997) 24 ECHR 523.
[198] *Kopp v Switzerland* (n 194), para 72.
[199] *Klass v Germany* (1979-80) 2 ECHR 214, paras 33-34.
[200] *Ireland v UK* (n 122) paras 239-240.
[201] Klass v Germany (n 199).

- as this makes it nearly - 'impossible for the applicants to show that any of their rights have been interfered with.'[202] This in turn poses a severe risk to the 'l'effet utile' of the Convention.[203] In agreement with the Commission in *Klass*, the ECtHR supported the deviation from the traditional application of Article 34 on the basis that the

> 'menace of surveillance can be claimed in itself to restrict free communication through postal and telecommunication services, thereby constituting for all users and all potential users a direct interference with the right guaranteed by Article 8.'[204]

Therefore, interception laws are capable of automatically engaging Article 8 based on their capacity to 'strike[s] at the freedom of communication between users of the telecommunications services…irrespective of any measures actually taken against them.'[205] The legacy of *Klass* means that applicants do not necessarily need to prove their communications have been intercepted, as it can suffice for them to show that it is possible they *may* have been subject to such measures.[206] Thus, the ECtHR in *Klass* viewed the potential for surveillance to alter the behaviour of individuals as harmful, rendering those at risk of surveillance as 'victims' for the purposes of engaging Article 8.[207]

However, the ECtHR has only relaxed Article 34 in a handful of cases and in other cases has applied the more stringent 'reasonable likelihood' test. For example, in *Halford v UK* the ECtHR examined the 'reasonable likelihood' that the applicant's telephone calls were intercepted. This was on the basis of Ms Halford's complaint that surveillance measures were actually applied to her as opposed to her Article 8 right

---

[202] *Klass v Germany* App no 5029/71 (Commission Decision, 9 March 1977) p 27.
[203] Ibid p 34.
[204] *Klass v Germany* (n 199) para 37.
[205] Ibid para 41.
[206] As seen in *Iordachi v Moldova* (2012) 54 ECHR 5, para 52, and *Liberty and others v UK* (n 167), para 57.
[207] This approach is also seen in the case of *Norris v Ireland* (1991) 13 ECHR 186 where the applicant (a homosexual male) was considered a 'victim' for the purposes of Article 25 enabling him to challenge the lawfulness of a piece of Irish legislation penalising buggery and acts of gross indecency between males, despite the law not being enforced against him. The impact of the law on the applicant's behaviour, however, was enough for him to be construed as a victim.

being 'menaced' by the mere existence of surveillance legislation as in *Klass*.[208] Accordingly, Ms Halford had to demonstrate the reasonable likelihood of her communications being intercepted in order for her claim to be deemed admissible by the Court, as opposed to merely pointing to the 'mere existence' of menacing surveillance legislation as in *Klass*. The reasonable likelihood test is, therefore, more difficult to fulfil than the 'mere existence' test.[209]

Thus, the ECtHR will not always deem the mere existence of surveillance legislation harmful to privacy, requiring in some cases that the applicant substantiate the harm caused. Consequently, Article 8 remains a highly individualistic right that is only typically accessible by natural persons. It is argued in Chapter 4 that this restriction of the scope of Article 8 is potentially damaging in the digital age where the bulk nature of surveillance makes it difficult to prove the concrete, personal harm caused by the mass gathering, processing, and retention of communications.

1.2 Processing

Processing is the second stage of surveillance and refers to the different ways in which gathered information has subsequently been used. There are a variety of different types of processing including the analysis and sharing of information. As shown below, the *potential* for processing can be enough to engage Article 8(1).

1.2.1 Potential for processing

Although wire-tapping constituted an automatic interference with Article 8(1) in *Malone v UK*, there was also extensive discussion on the practice of 'metering.'[210] 'Metering' is the process by which the Post Office was able to ensure correct billing through the use of a device which registered the numbers dialled, time, and duration of phone calls.[211] The applicant argued that this process was also an interference with private life and one that was unlawful given that no legislation existed permitting its

---

[208] *Halford v UK* (n 197) para 48.
[209] As also concluded by Bart van der Sloot in 'How to assess privacy violations in the age of Big Data? Analysing the three different tests developed by the ECtHR and adding for a fourth one' (2015) 24 Information & Communications Technology Law 74.
[210] *Malone v UK* (n 195) para 84.
[211] Ibid paras 56 and 83.

use.[212] However, the ECtHR, in highlighting the billing purposes of metering, proceeded to distinguish it from interception on the basis that: (i) the Post Office 'made use only of signals sent to itself' and, (ii) it was not 'undesirable and illegitimate in democratic society.'[213] The Court's distinction between metering and interception agrees with the definition of information gathering in Chapter 1, where it was argued that the gathering of information for a specific purpose (and every piece of that information being used for that purpose) did not constitute surveillance. Accordingly, the ECtHR rightly found that the the act of metering did not, in itself, interfere with the applicant's private life like wire-tapping.[214]

However, the ECtHR went on to find that the subsequent sharing of metering information to police without the subscriber's knowledge or consent *did* constitute an interference with Article 8(1).[215] The Court based its finding on the subsequent *potential* for processing by police for purposes of a criminal investigation - which strayed significantly from the original purpose for which the data was gathered.[216] Thus, the *potential* for processing arising upon the sharing of records served to transform the nature of metering from benign information gathering into an exercise of surveillance capable of engaging Article 8(1).[217]

1.2.2 Foreseeability of processing

The reasoning behind the ECtHR's emphasis on processing is illustrated in *Peck v UK* where the applicant was captured attempting to commit suicide on CCTV, the footage of which was then shared with the media who proceeded to broadcast the images.[218] The government claimed that neither the recording of the applicant trying to commit suicide on a public street, nor the subsequent disclosure of the footage to the media engaged Article 8(1) given the very public nature with which the applicant decided to

[212] Ibid para 59.
[213] Ibid para 84.
[214] Ibid.
[215] ibid.
[216] This finding was upheld in the case of *PG and JH v UK* (n 188) paras 42-43.
[217] *Malone v UK* (n 195) paras 83-84.
[218] *Peck v UK* (n 23).

act.[219] In reaching the conclusion that the disclosure of the relevant footage amounted to an interference with private life,[220] the ECtHR first underlined an earlier Commission decision which found that unrecorded CCTV does not amount to an interference with private life on the basis that there exists no potential for future processing.[221] However, upon the creation of a permanent record, such potential does arise. At the crux of its judgment in *Peck*, the ECtHR underlined the subsequent unforeseen *use* of the footage for broadcasting which surpassed 'that which the applicant could possibly have foreseen when he walked in Brentwood.'[222]

Peck v UK thus demonstrates the ECtHR's emphasis on the processing of information, as well as the extent to which the foreseeability of such processing will influence the ECtHR's finding of an interference with private life. *Peck* also demonstrates that, while limited, an expectation of privacy does exist in public and can be triggered by the creation and unforeseen processing of records containing information related to one's private life. This is further illustrated in the case of *Friedl v Austria*, below. [223]

1.2.3 Restrictions on processing

In *Friedl v Austria*, it was claimed that the taking and retention of photographs of the applicant participating in a public demonstration interfered with his right to private life under Article 8.[224] However, it was held by the Commission that the purpose for which the photographs were taken (to record the character of the demonstration) together with the applicant's voluntary participation in the public event, rendered his Article 8 claim inadmissible.[225] Fundamental to the Commission's judgment, was that the photographs were set to be destroyed by a specific date and that the anonymity of those photographed was maintained.[226] *Friedl* thus demonstrates that a limited expectation

[219] Ibid para 53.
[220] Ibid para 63.
[221] *Herbecq v Belgium* 32200/96 and 32201/96 (Commission Decision, 14 January 1998), DR 92-B, para 59.
[222] Ibid paras 60-63.
[223] Friedl v Austria (n 185).
[224] Ibid.
[225] Ibid paras 49-51.
[226] Ibid para 50.

of privacy exists in public and that restrictions mitigating the authorities' processing power will limit the scope for an Article 8 claim to be made.[227]

Peck and *Friedl* show that whilst there is a reduced expectation of privacy in public, the subsequent processing of information maintains a gateway into Article 8, despite the (quasi-) participatory or public nature of one's actions. This shows an acknowledgement on behalf of the ECtHR that expectations of privacy can and do exist outwith traditionally private spaces, albeit to a limited extent. This is a particularly important acknowledgement in today's contemporary surveillance landscape (where sharing online (eg on social media) has become an integral aspect of the culture of surveillance participated in by individuals for the purposes of sociality) as it enables expectations of privacy to persist in realms of exposure and provide protection against surveillance regimes aimed at the sweeping up of this (semi-) public information. The extent to which the IP Act aligns with the ECtHR in this respect - and thus provides adequate protection to privacy within the contemporary surveillance landscape - is examined in Chapter 5 via an analysis of its bulk powers under Article 8 ECHR.

1.3 Retention

This section examines the engagement of Article 8(1) upon the retention of material.[228] The ECtHR has consistently held that the retention of information relating to an individual's private life by a public authority interferes with privacy.[229] For example, in *Leander v Sweden* an individual had been refused employment as a museum technician on the basis of personal information held about him in a secret police register.[230] It was held that 'both the storing and release of such information amounted

---

[227] This is also seen in the domestic case of *R (on the application of Catt) and R(T) v Association of Chief Police Officers of England, Wales and Northern Ireland* [2015] UKSC 9, where it was held that the retention of photographs of Catt's participation in protests on a searchable database interfered with Article 8(1) as the data was not anonymized and it was unclear how long it was to be stored on the database. (The case of Ms. T concerned the storage of information on a minor altercation with her neighbor but this is not relevant to this thesis and is not, therefore, relevant).

[228] Note that 'retention' and 'storage' are used interchangeably in this section.

[229] *Leander v Sweden* (1987) 9 ECHR 433; *Amann v Switzerland* (2000) 30 ECHR 843; *Rotaru v Romania* (2000) 8 BHRC 449.

[230] Nb the museum was next to a naval base and, therefore, in a military protected zone so all employees were subject to a personnel control check against the register.

to an interference with his right to respect for private life.'[231] The following thus establishes the ECtHR's definition of 'information relating to private life.'

1.3.1 Information relating to private life

As stated above, the ECtHR operates on a particularly broad understanding of 'private life,' including: the physical and psychological integrity of a person; information about a person's health or ethnicity; and, a right to personal development. It follows that Article 8(1) can be engaged by the retention of many different types of information.

There have been attempts to restrict the type of information capable of engaging Article 8(1) to 'sensitive information,' as seen in the case of *Amann v Switzerland* regarding the retention of information on the applicant's business by Swiss authorities.[232] The government argued that an interference had not occurred on the basis that: (i) the card did not contain 'sensitive' information; (ii) the applicant had not been inconvenienced by its retention, and; (iii) it had likely never been used by a third party.[233] However, the ECtHR found that an interference *had* occurred on the basis that: (i) it was not for the court to speculate what constituted 'sensitive' information, it merely had to relate to the individual's private life, and; (ii) retention of such information amounts to an interference regardless of whether or not it was used.[234] *Amann* thus demonstrates that the retention of information relating to private life engages Article 8(1) regardless of whether or not the concerned material is 'sensitive' or subsequently processed.

The ECtHR's approach to establishing whether information relates to private information was clarified in the case of *S and Marper v UK* regarding the retention of cellular samples, DNA profiles and fingerprints under English and Welsh law.[235] The

---

[231] *Leander v Sweden* (n 229) para 48.
[232] Amann v Switzerland (n 229).
[233] Ibid para 68.
[234] Ibid para 69.
[235] *S and Marper v UK* (2009) 48 ECHR 50. Criminal Justice and Police Act 2001, s 82. This was contrasted to the Scottish system of DNA retention under s 18(3) of the Criminal Procedure Act of Scotland 1995 where DNA samples and resulting profiles must be destroyed if the individual is not convicted or is granted absolute discharge. However, if suspected of sexual or violent offences biological samples and profiles may be retained for three years under s 83 of the Police, Public Order

ECtHR held that, in order to establish that the concerned data relates to private life, due regard must be given to: the specific context in which the information has been recorded and retained; the nature of the records; the way in which the records are used; and, the results that may be obtained from such processing.[236] The ECtHR went on to conclude that the retention of the concerned data *did* interfere with Article 8(1) on the basis that: (i) there was significant potential for processing; (ii) very sensitive information was contained within the records (i.e. health and genetic code); and, (iii) persons could be identified from the records via automated processing techniques.[237]

Thus, in establishing the relationship of the data to private life, the ECtHR focussed on the potential processing of the data and on what sensitive and private information might be revealed through such practices. This approach subsequently enabled the Court to reject the government's claim that the relevant data 'contained no materially intrusive information about an individual or his personality' because the form in which they were stored (sequences of numbers and code) did not provide information about a person's activities without further processing.[238]

The ECtHR's emphasis on the *potential* for information to relate to private life thus provides a broad remit for claims against the retention of information under Article 8(1). This is particularly useful in the digital age where facts about our lives, personalities, activities, and relationships can be derived from data that, singularly, might not contain any 'materially intrusive information' but when aggregated into vast, searchable databases, can become incredibly revelatory and have a significant impact on the private life of the individual.[239]

1.3.2 Retention of public information

The above sections have demonstrated that the retention of information relating to, or capable of relating to, private life will engage Article 8(1). This section examines

---

and Criminal Justice (Scotland)Act 2006. The system in Northern Ireland regarding the retention of DNA and fingerprints mirrors England and Wales.

[236] *S and Marper v UK* ibid para 67.

[237] Ibid paras 68-86.

[238] Ibid para 65.

[239] See Chapter 4, Part 2, section 1.2.3.

whether the retention of public information is capable of engaging Article 8 via an examination of *Rotaru v Romania.*[240]

Rotaru concerned the state's retention of 'false and defamatory' information on the applicant's involvement in campaigns against the previous Communist regime. The government claimed that the applicant's participation in political activities waived any right to anonymity that was inherent to private life.[241] However, the ECtHR upheld the applicant's claim on the basis that: (i) the information was systematically collected and stored by authorities, and (ii) the information was historical.[242] Thus, despite the public nature of the concerned material, the way in which the information was retained served to engage Article 8(1).[243] *Rotaru* may thus be viewed as creating a gateway into Article 8 for the surveillance of public information. This bears especial relevance in the contemporary surveillance landscape where vast swathes of data, both public and private, are continuously and systematically retained by states and corporations. This is demonstrated in Chapters 3 and 4.

Having established the different ways in which surveillance is capable of engaging Article 8(1), the following section examines the ECtHR's approach to determining the justifiability of interferences with private life. This will begin with an overview of the legality test before going on to examine its application by the ECtHR in its surveillance jurisprudence.

2 The legality of interferences

Having established that an interference exists, the ECtHR must determine its legality under Article 8(2) which states that

[240] Rotaru v Romania (n 229).
[241] Ibid para 42.
[242] Ibid paras 43-44.
[243] This is also seen in the domestic case of *Catt* (n 227), where the systematic retention of historical information on a searchable database was held to interfere with Article 8(1) (albeit lawfully based on the circumstances of the case).

> ‘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.’

This section will focus on the ECtHR’s application of the ‘in accordance with law’ requirement in its surveillance case law. The necessity and proportionality requirements are examined in section 3, below.

2.1 The legality test

The general meaning of ‘in accordance with law’ was established in *Sunday Times v UK* where the ECtHR considered the obligations flowing from the term ‘prescribed by law.’[244] The Court established that ‘prescribed by law’ ‘covers not only statute but also unwritten law’ and held that two requirements flow from the term: (i) accessibility, and (ii) foreseeability.[245] Accessibility is required for the individual to be able to have an indication as to what legal rules might apply to a particular circumstance. Foreseeability requires the law to be drafted with sufficient precision that the citizen can reasonably foresee the consequences of his actions.[246]

Furthermore, in *Malone v UK* the ECtHR held that the legality requirement of Article 8(2) also, ‘relates to the quality of the law, requiring it to be compatible with the rule of law’ to safeguard against arbitrary interferences with private life by public authorities.[247] The Court went on to stress the fundamental importance of the quality of law within the context of covert surveillance as the implementation of such measures are not open to public scrutiny. Accordingly,

> ‘the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure

---

[244] *The Sunday Times v UK* (1979) 2 ECHR 245, para 48. Note that ‘prescribed by law’ derives from the French phrase ‘prévues la loi’ and is used interchangeably with ‘in accordance with law,’ the latter of which will be used in this thesis for consistency.
[245] Ibid paras 47 and 49.
[246] Ibid para 49.
[247] *Malone v UK* (n 195) para 67.

> in question, to give the individual adequate protection against arbitrary interference.'[248]

The 'in accordance with law' requirement thus reflects the general rule of law principle that 'the law should conform to standards designed to enable it effectively to guide action' so that people have a solid legal basis upon which to make informed choices about how they live their lives.[249] It follows that granting unrestricted discretionary power to a public authority runs contrary to the rule of law as it allows for arbitrariness and unpredictability which frustrates the individual's ability to plan their lives in accordance with the law.[250]

The legality test is made up of three limbs: (i) basis in domestic law; (ii) accessibility and foreseeability, and; (iii) sufficient safeguards against arbitrary treatment. The following assesses the ECtHR's application of each within its surveillance case law. The legality of certain powers in the IP Act are subsequently determined according to their adherence to these principles in Chapter 5.

2.1.1. Basis in domestic law

As established above, interception is the only type of surveillance capable of automatically engaging Article 8(1) at the gathering stage. Consequently, in cases involving interception the ECtHR must always go on to assess the legality of the practice under Article 8(2). First, the Court will have to determine whether the interference has a basis in domestic law before going on to assess whether the law is sufficient in terms of its accessibility, foreseeability, and safeguards. This first branch of the legality test is not usually contentious as states possess a basic awareness of the need to regulate interferences with human rights.

---

[248] Ibid 68.
[249] Joseph Raz, *The Authority of Law* (Oxford, 1979) 218. See also *Entick v Carrington* (1765) 19 St Tr 1029 where it was held that the state cannot override the rights of the individual without legal authority to do so
[250] Raz ibid 216-218.

Although, in *Malone v UK* the wire-tapping and processing of metering records was found to lack any basis in domestic law.[251] Whilst the ECtHR acknowledged that 'detailed procedures concerning interception of communications on behalf of the police in England and Wales do exist' - it went on to hold that

> 'it cannot be said with any reasonable certainty what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive' [– and as such -] 'the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking.'[252]

Thus, whilst the procedure for wire-tapping was set out elsewhere - in a committee report[253] and government White Paper[254] - because these documents were not legally binding, wire-tapping could not be deemed 'in accordance with law.'[255] This was also found in relation to the processing of metering records.[256]

In response to the above judgment, the Interception of Communications Act 1985 was passed to regulate the interception of postal and telephonic communications. Despite being widely criticised for its significant shortcomings (eventually being replaced by RIPA 2000), the Act signified an important recognition by UK law-makers of threats to private life by interception, albeit begrudgingly.[257]

---

[251] *Malone v UK* (n 195).
[252] Ibid para 79.
[253] Birkett Committee, *Report of the Committee of Privy Councillors Appointed to Inquire into the Interception of Communications* (Cmnd 283, 1957) ('Birkett report') The Birkett Committee was established to 'consider and report upon the exercise by the Secretary of State of the executive power to intercept communications and, in particular, under what authority, to what extent and for what purposes this power has been exercised and to what use information so obtained has been put; and to recommend whether, how and subject to what safeguards, this power should be exercised…'
[254] Home Office, The Interception of Communications in Great Britain (Cmnd 7873, 1980).
[255] *Malone v UK* (n 195) para 79.
[256] Ibid para 87.
[257] See 75 HC Deb 151 (12 March 1985). See also *R v Preston* [1994] 2 AC 130, [148] where Lord Mustill described IOCA as a 'short but difficult statute,' and *Halford v UK* (n 197) para 51 where the ECtHR condemned the narrow scope of the Act which failed to govern wider aspects of covert surveillance like non-public telephones. See also Adam Tomkins, 'Intercepted Evidence: Now You Hear Me, Now You Don't' (1994) 57 Modern Law Review 941.

2.1.2. Accessibility and Foreseeability

Although the Court's main emphasis in *Malone v UK* was placed on the existence of domestic law, or lack thereof, the accessibility and foreseeability requirements were also considered. The ECtHR acknowledged the need to adapt the application of these branches of the legality test in surveillance cases. This was especially regarding foreseeability which the Court held, 'cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly.'[258] The ECtHR thus recognises the legitimacy of covert surveillance and the subsequent need to adapt the foreseeability requirement accordingly. However, it went on to state that sufficient clarity was still required in order for citizens to be provided with an adequate indication as to the circumstances in which public authorities are permitted to resort to such practices.[259]

Through an examination of relevant case law, the following establishes the characteristics of surveillance legislation that the ECtHR has deemed integral to the fulfilment of the accessibility and foreseeability requirements in the context of surveillance.

2.1.2.1 Scope of discretionary power

In the aforementioned case of *Amann v Switzerland*, in assessing whether the concerned wire-tapping was in accordance with law, the ECtHR denounced the relevant law for failing to give any 'indication as to the persons concerned by such measures, circumstances in which they may be ordered, means to be employed or the procedures to be observed.'[260] Furthermore, in relation to the creation, use, storage, and destruction of files containing the gathered information, it was held that the lack of precision with which the necessary rules governing the file's creation, storage, and destruction were drafted, did not fulfil the accessibility and foreseeability standards as

[258] *Malone v UK* (n 195) para 67. Upheld most recently in the case of *Zakharov v Russia* (n 204).
[259] Ibid.
[260] *Amann v Switzerland* (n 229) para 58.

it failed to establish the 'scope and conditions of exercise of the authorities' discretionary power.'[261]

The ECtHR's emphasis on the scope of discretionary power is also seen in *Huvig v France* and *Kruslin v France*.[262] In both cases, the Court underlined the dangers posed by interception and the subsequent need for this practice to 'be based on a "law" that is particularly precise' [- adding -] 'it is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.'[263] The ECtHR went on to list specific safeguards that ought to have been included in the law.[264] This not only demonstrates the Court's views on interception as a particularly serious interference with Article 8, but so too, its awareness of multiplying unknowns - or what Donald Rumsfeld might refer to as 'known unknowns' - arising from perpetual advances in technology that make it difficult for the law to keep pace.[265]

Whilst the ECtHR evidently places a strong emphasis on the precision of law when defining the scope of surveillance powers, it has also recognised that specificity of language carries its own risks, such as the creation of lacunae through which new surveillance technologies and practices can thrive. This was recently acknowledged in the case of *Szabo and Vissy v Hungary* where the Court noted that:

> 'to avoid excessive rigidity and to keep pace with changing circumstances […] many laws are inevitably couched in terms which, to a greater or lesser extent, are vague.'[266]

Therefore, a delicate balance must be struck between vague and precise language when defining the scope of surveillance powers.

---

[261] Ibid, para 62.
[262] *Kruslin v France* (1990) ECHR 547; *Huvig v France* (1990) 12 ECHR 528.
[263] Ibid para 33 and para 32.
[264] Ibid para 35 and para 34. Safeguards are discussed in section 2.1.4 below.
[265] Donald Rumsfeld (Nato Press Conference, Brussels, 6 June 2002) <http://www.nato.int/docu/speech/2002/s020606g.htm> accessed 27 April 2016.
[266] *Szabó and Vissy v Hungary* (2016) 63 ECHR 3, para 64.

2.1.2.2 Soft law

When assessing the foreseeability of legislation, the ECtHR will take into consideration accompanying soft law, such as non-legal instructions and regulations. This is seen in the aforementioned case of *Leander v Sweden* where the ECtHR held that when assessing foreseeability, account may be had of 'instructions or administrative practices which do not have the status of substantive law, in so far as those concerned are made sufficiently aware of their contents.'[267] *Leander* thus represents an acknowledgment on behalf of the ECtHR as to the limitations of substantive law in covering every possible eventuality and the utility of soft law for further informing the individual as to when and how a particular measure might be used. This is particularly useful within the context of the fast-paced technological climate as it enables the foreseeability requirement to be fulfilled without laws having to become overly technical or rigid.[268] Although breaches of soft law do not have legal repercussions, significant consequences can still arise which act as a deterrence to malpractice.[269]

Soft law is thus rightly taken into consideration by the ECtHR when determining the foreseeability of an interference. It is not only instrumental in providing more detailed information to individuals and public authorities on the permitted uses and practices of surveillance, but it also enables the law to remain technologically neutral and to avoid excessive rigidity.[270] However, as also stipulated by the ECtHR in *Leander,* soft law cannot substitute necessary primary legislation, with the law itself having to indicate the scope of any discretion conferred on a public authority with sufficient clarity to safeguard against arbitrariness.[271] Thus, soft law can only act as an

---

[267] *Leander v Sweden* (n 229) paras 47 and 51.
[268] As noted in *Silver and others v UK* (1983) 5 ECHR 347, para 88.
[269] As demonstrated by the Codes of Practice accompanying the Police and Criminal Evidence Act 1984 ('PACE' and 'PACE codes'). Whilst a breach of the Codes cannot result in criminal or civil proceedings (PACE, s 67(10)), it can lead to the refusal of evidence by a court, quashed convictions, and disciplinary proceedings (these consequences can arise pursuant to PACE, s 67(11)).
[270] Although, the benefits of technologically neutral laws are debated. For example, Sir David Omand argues that this approach results in overly complex laws that are difficult for the average layperson to understand, such as RIPA 2000, see Home Affairs Committee: Evidence, *Counter-terrorism 17th Report*, (2013-14, HC231), Q589.
[271] *Leander v Sweden* (n 229), para 51. This is supported in the cases of *Khan v UK* (2001) 31 ECHR 45, para 27, and *PG and JH v UK* (n 188) paras 37-38, where it was held that Home Office guidelines

accoutrement to, as opposed to substitution for, the primary legislation that must at least define the scope of discretion conferred.[272]

2.1.4 Sufficient safeguards and oversight

In light of the covert nature of surveillance, the ECtHR has consistently warned against the risk of arbitrariness and abuse of power in this area. Consequently, it places significant emphasis on the incorporation of sufficient safeguards into state surveillance laws.[273] The following demonstrates that the Court has been fairly prescriptive regarding the types of safeguards required for laws governing interception and equally intrusive surveillance practices.

2.1.4.1 Strict safeguard principles

In *Kruslin* and *Huvig*, the ECtHR established that each of the following must be clearly defined in law to ensure foreseeability: (i) categories of people likely to have their phones tapped; (ii) the nature of offences likely to trigger this measure; (iii) judicially imposed limits on the duration of phone tapping; (iv) a prescribed method for drawing up summary reports; (v) procedures and safeguards for sharing the records, and; (vi) procedures for the destruction or erasure of records (particularly where the individual has been acquitted or discharged of the concerned offence).[274]

Murphy notes the lucidity of the ECtHR's guidance, commenting that it 'is striking and appears to demand that domestic legislators regulate their surveillance activities

---

on the use of covert listening devices did not fulfil the legality requirement under Article 8(2) as 'there existed no statutory system to regulate the use of covert listening devices.'

[272] The cases of *Khan* and *PG and JH* may, however, be contrasted with the recent case of *Roman Zakharov v Russia* (n 204), in which an Order permitting the mass interception of communications had only been permitted twice: once in a Ministry of Communications' magazine (available only through subscription); and, once on a privately-maintained legal database. However, the ECtHR held that whilst the narrow publication of the order was 'regrettable,' it was still accessible for the purposes of Article 8(2). Although, this may simply have been due to the Court's desire to focus on the foreseeability and necessity of the concerned practice, at para 242.

[273] See: Klass v Germany (n 23), para 55; Kopp v Switzerland (n 194), para 72; Valenzuela-Contreras v Spain (1999) 28 ECHR 483; Kruslin v France (n 262); Huvig v France (n 262).

[274] *Kruslin v France* (n 262) para 35; *Huvig v France* (n 262) para 34. Also subsequently upheld in *Valenzuela Contreras v Spain* (n 273) para 46. See also, *Weber and Saravia v Germany* (2006) ECHR 1173 para 95.

in a circumscribed manner.'[275] Murphy is supported by the case of *Liberty and others v UK* regarding the bulk interception of communications between the UK and Ireland from 1990 to 1997 under the Interception of Communications Act 1985.[276] The Court's main focus was placed on section 3(2) which allowed the Secretary of State to issue interception warrants for external communications. Despite section 6(1) requiring that the Secretary of State 'make such arrangements' as he deems necessary to ensure that intercepted material not authorised by the warrant was not read or listened to, such 'arrangements' were held to lack the necessary publicity required for the individual to scrutinise whether or not they had been followed.[277]

Furthermore, despite the intercepted material being electronically searched in order to restrict the number of domestic communications listened to or read by analysts, it was found that the search terms were so broad and vague that the effectiveness of this safeguard was significantly reduced.[278] The ECtHR thus held that the applicants' Article 8 right had been unlawfully interfered with on the basis that IOCA failed

> 'to provide with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications.'[279]

Liberty and others v UK demonstrates that the mere existence of safeguards will not suffice to fulfil the legality requirement as the ECtHR will also examine their effectiveness.

2.1.4.2 General safeguard principles

The ECtHR's application of the stricter safeguard principles depends on the surveillance concerned. For example, it would be unnecessarily cumbersome to

---

[275] Maria Helen Murphy, 'A shift in the approach of the European Court of Human Rights in surveillance cases: a rejuvenation of necessity?' (2014) European Human Rights Law Review 507, 509.
[276] Liberty and others v UK (n 167).
[277] Ibid para 66.
[278] Ibid.
[279] Ibid para 69.

require judicial authorisation for low-level surveillance, like unrecorded CCTV, where only a snapshot of the subject's life is viewed for a limited period of time.

This is seen in *Uzun v Germany* where the ECtHR held that the use of a GPS-tracker on a car ought to be distinguished from

> 'other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings.'[280]

Accordingly, the Court went on to hold that in cases regarding less serious interferences with private life, 'the strict standards, set up and applied in the specific context of surveillance of telecommunications,' are not applicable.[281] Instead, it applied 'more general principles on adequate protection against arbitrary interference,' - including - 'the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.'[282]

The ECtHR can thus be seen to look for a layering of information when determining how stringently to assess the safeguards of surveillance legislation, with fewer safeguards being required for less intrusive surveillance practices (or rather, what the Court considers to be less intrusive surveillance). As shown in section 3.3, below, this is also the approach taken by the Court when determining the margin of appreciation awarded to states in surveillance cases. However, it is questionable how appropriate this approach is in the contemporary surveillance landscape. Chapter 3 shows that significant value can be derived from communications data (the who, what, when, where of a communication as opposed to its content) with vast amounts of information about one's life capable of being revealed upon its collection, aggregation, and processing. However, as shown in Chapter 5, the surveillance of communications data

[280] *Uzun v Germany* (2011) 53 ECHR 24, para 52.
[281] Ibid para 66.
[282] Ibid para 63.

falls outwith the definition of interception which is content-focussed and thus fails to trigger the stricter safeguard principles set out above. Although, in the recent case of *RE v UK* the ECtHR held that the sufficiency of safeguards was to be determined according to 'the level of interference with an individual's right to respect for his or her private life and not the technical definition of that interference.'[283] This approach could, therefore, lead to the application of the stricter principles to a wider variety of surveillance practices.

2.1.4.3 Oversight

In *Klass v Germany* it was considered whether judicial oversight had to be included in surveillance laws.[284] The ECtHR demonstrated a preference for judicial oversight, noting that 'it is in principle desirable to entrust supervisory control to a judge' given the risk of arbitrariness in the surveillance context.[285] However, it concluded that a lack of judicial oversight was not unlawful in terms of Article 8(2) as those overseeing the system were, 'independent of the authorities carrying out the surveillance, and vested with sufficient powers and competence to exercise an effective and continuous control.'[286] Similarly, in the aforementioned case of *Szabo and Vissy v Hungary*, the ECtHR emphasised the desirability of supervisory control being carried out by a judge given that the, 'political nature of the authorisation and supervision increases the risk of abusive measures.'[287] However, it added that an 'independent body over the issuing body's authority'[288] would also be acceptable as judicial authorisation would not always be feasible, particularly in light of 'the present-day upheaval caused by terrorist attacks.'[289]

Thus, whilst the ECtHR has a preference for judicial oversight, emphasis is placed on the impartiality and independence of the oversight as opposed to its formal constitution. This approach is in line with the June 2014 report of the Office of the UN

---

[283] *RE v UK* (2016) 63 ECHR 2, para 130.
[284] *Klass v Germany* (n 23) para 54.
[285] Ibid.
[286] Ibid para 56.
[287] Szabó and Vissy v Hungary (n 266) para 77.
[288] Ibid.
[289] Ibid, para 80.

High Commissioner for Human Rights (OHCHR) which recommended an oversight model combining parliamentary, administrative, and judicial oversight on the basis that,

> 'judicial warranting or review of the digital surveillance activities of intelligence and or/law enforcement agencies have amounted effectively to an exercise in rubber-stamping.'[290]

Thus, whilst we tend to view judicial oversight as the gold standard it has often amounted to little more than blind endorsement. As in section 2.1.4.1, above, it is the effectiveness of the practice that should matter rather than just its form.

Chapter 5 examines the sufficiency of the oversight under the IP Act which introduces a 'double-lock mechanism' requiring both ministerial and judicial authorisation of surveillance warrants.[291] Whilst this would appear to fulfil the above standards and preferences of the ECtHR and OHCHR by incorporating judicial involvement, question marks over the effectiveness and independence of the regime emerge from loopholes in its application.[292]

3 Justified interferences

Having established the legality of an interference, the ECtHR will go on to consider whether the concerned surveillance pursues a legitimate aim and is necessary in a democratic society. The legitimate aims listed under Article 8(2) include: national security; public safety; economic wellbeing of the country; prevention of disorder or crime; protection of health or morals; and, the protection of the rights and freedoms of others. Typically, the ECtHR grants a wide margin of appreciation to the state regarding the existence of a legitimate aim, particularly in surveillance cases where the interference is typically aimed at safeguarding national security or the prevention

---

[290] OHCHR, *The Right to Privacy in a Digital Age* (June 30, 2014), 12-13 <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf> accessed 2 November 2016.
[291] See Chapter 5, section 2.2.1.3.
[292] Concerns raised over both pre-authorisation and post-inspection of warrants being carried out by Judicial Commissioners (meaning the same body is essentially overseeing itself) in Joint Committee on Human Rights, *Legislative scrutiny; investigatory powers bill* (2016-17, HL 6, HC 104) Part 8.

of crime.[293] Consequently, the ECtHR tends to focus on the necessity and proportionality of an interference.

The following categorical approach to the examination of the 'necessary in a democratic society' requirement has been adopted: (i) defining 'democratic necessity;' (ii) proportionality; and, (iii) margin of appreciation. Whilst the ECtHR does tend to break the test down into these three categories, perhaps because there is such a significant degree of overlap between them, this approach has been adopted here for the purposes of clarity.

3.1 Defining 'democratic necessity'

In *Lingens v Austria* the ECtHR defined 'necessary' as implying the existence of a 'pressing social need,' and noted that whilst states enjoy a margin of appreciation as to whether such a need exists, it remains subject to ECtHR supervision.[294] In *Handyside v United Kingdom*, the ECtHR held that the meaning of 'necessary' lay somewhere in-between 'indispensable' and more flexible terms like: 'admissible,' ordinary,' 'useful,' 'reasonable,' and 'desirable.'[295] The Court has also indicated that, in relation to rights like Article 6 (the right to fair trial)[296] and Article 10[297] which are integral to democratic society, restrictions listed under paragraph 2 are to be construed narrowly. 'Pluralism, tolerance, and broad-mindedness' have also been heralded by the Court as fundamental to democratic society.[298] Aside from this guidance, the ECtHR has largely refrained from giving an explicit definition of 'necessity' or prescribing a list of the needs of democratic society, leaving 'the content of the "democratic necessity test" to remain highly fluid and indeterminable.'[299]

---

[293] It is widely accepted that a wide margin of appreciation exists in matters of national security. See, Steven Greer, *The margin of appreciation: interception and discretion under the European Convention of Human Rights* (Council of Europe, 2000); Yutaka Arai-Takahashi, *The margin of appreciation doctrine and the principle of proportionality in the jurisprudence of the ECHR* (Intersentia, 2002) 104-107.
[294] *Lingens v Austria* (1986) 8 ECHR 407, para 39.
[295] *Handyside v UK* (1979-80) 1 ECHR 737, para 48.
[296] *Delcourt v Belgium* (1979-80) 1 ECHR 355, para 25.
[297] *Handyside* (n 290), para 49.
[298] Ibid para 49.
[299] Stephen Greer, 'The exceptions to Articles 8 to 11 of the European Convention of Human Rights'

Accordingly, only limited guidance on the definition of democratic necessity within the context of surveillance can be drawn from the case law. For example, the ECtHR evidently accepts a basic need for surveillance within democratic society, as demonstrated in *Klass v Germany*, where it accepted that covert surveillance had become necessary in light of threats to national security from 'highly sophisticated forms of espionage and by terrorism.'[300] However, the Court went on to state that this does not grant states with an unlimited area of discretion and so they, 'may not, in the name of struggle against espionage and terrorism, adopt whatever measures they deem appropriate.'[301]

Aside from this, however, the ECtHR has provided little other guidance on the need for surveillance within democratic society. Instead, it has tended to approach the issue of necessity as a question of proportionality. This has led to significant overlap between the two tests with Professor McHarg querying whether the 'the nature of democratic necessity [is] distinct from or part of the assessment of proportionality.'[302]

3.2 Proportionality

Whilst 'proportionality' is not explicitly referenced in the text of the ECHR, it is visible in a 'thinly veiled form'[303] within the judgments of the ECtHR where the principle of proportionality has been hung upon the 'textual peg' of the 'necessary in a democratic society' requirement.[304] Proportionality has become a fundamental tool for regulating the application and protection of Convention rights. This is noted by Barak who argues that, 'constitutional rights are relative – there is justification for not realising them to the full extent of their scope. The criterion by which such a realisation

---

in *Human Rights Files no.15* (Council of Europe Publishing, 1997).
[300] *Klass v Germany* (n 199) para 48.
[301] Ibid, para 49.
[302] Aileen McHarg, 'Reconciling human rights and the public interest: Conceptual problems and doctrinal uncertainty in the jurisprudence of the European Court of Human Rights' (1999) 62 The Modern Law Review 671, 688.
[303] Marc-Andre Eissen, 'The principle of proportionality in the case-law of the European Court of Human Rights' in Ronald Macdonald, Franz Matxcher and Herbert Petzold (eds) *The European system for the protection of human rights* (Kluwer Academic Publishers, 1993) 125.
[304] Julian Rivers, 'Proportionality and variable intensity of review' (2006) 65 The Cambridge Law Journal 174, 177.

is measured is that of proportionality.'[305] Proportionality has thus come to be described as the 'methodological tool' used to test the justification for limiting a Convention right.[306]

Although states like the UK have attempted to infuse the proportionality test with a sense of structure,[307] a 'one-stop-shop' proportionality test does not exist. The intensity of review depends upon a variety of different factors, including: the facts of the case, the right involved, and the nature of the interference in question.[308] Whilst such flexibility is necessary given that not all rights or interferences will justify the same intensity of review as others,[309] the extent to which this flexibility varies has led to considerable criticism by commentators and the judiciary. Chan, for example, argues that, 'proportionality has been presented as if it is a magic wand that can shrink or expand flexibly at the court's will.'[310]

The following examines the ECtHR's application of the proportionality test in its surveillance jurisprudence as means of establishing the standard of review typically applied in this context. This standard is subsequently used in Chapter 5 to argue that the IP Act's failure to recognise the role of the individual in the contemporary surveillance landscape has led to the introduction of disproportionate surveillance powers.

3.2.1 Proportionate surveillance

Generally, in surveillance cases a breach of the 'in accordance with law' requirement will 'obliterate the need for evaluations based on the third standard, save in very

---

[305] Aharon Barak, Proportionality: Constitutional rights and their limitations (Cambridge University Press 2012) 131.
[306] Ibid.
[307] See, for example, R (on the application of Daly) v Secretary of State for the Home Department [2001] UKHL 26, [27]-[28] where the court implemented the 3-stage 'de Freitas' formula from de Freitas v Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing [1999] 1 AC 69 the Privy Council.
[308] *Kennedy v United Kingdom* (2011) 52 ECHR 4, para 155.
[309] Mark Elliott, 'The HRA 1998 and the standard of substantive review' (2002) 7 JR 97, 99.
[310] Cora Chan, 'Proportionality and invariable baseline intensity of review' (2013) Legal Studies 1, 2. See also, Bart van der Sloot who questions the suitability of the proportionality test within the 'Big Data' era, see van der Sloot (n 209), 99.

special circumstances where the nature of issues relating to these standards is such as to require examinations in conjunction.'[311] The ECtHR's apparent preference for the legality test and resulting neglect of the proportionality principle in this area has been the subject of criticism by both commentators and judges.[312]

Where the ECtHR *has* gone on to examine the proportionality of a practice it has tended to do so pragmatically. It tends to adopt a procedural approach by focussing largely on the existence of adequate and effective safeguards, avoiding an in-depth analysis of the balancing aspect of the proportionality test (ie whether the interference outweighs the harm caused to the affected rights) otherwise known as the *proportionality strictu sensu* branch of the test.[313] Consequently, the ECtHR's assessment of the necessity requirement in surveillance cases can look more like an extended discussion of the 'quality of law' requirement as opposed to a structured analysis of proportionality.[314]

This approach enables the ECtHR to avoid making seemingly arbitrary judgments based on 'intuition and improvisation'[315] and interfering 'with questions that they lack the institutional capacity or democratic legitimacy to decide.'[316] However, this procedural approach to necessity is also problematic as it leaves relatively little room for meaningful analysis on the proportionality of surveillance measures. An exception to this trend is seen in the aforementioned case of *S and Marper v UK* where the

---

[311] Van Dijk, van Hoof, van Rijn, and Zwaak, *Theory and Practice of the European Convention on Human Rights* (4th edn, Intersentia, 2006) 335.
[312] See, for example, Moreham (n 183) 55-56; Rita Esen 'Intercepting communications 'in accordance with the law' (2012) 76 Journal of Criminal Law 164, 164; Stefan Sottiaux, *Terrorism and the limitation of rights: The ECHR and the US constitution* (Hart publishing, 2008) 276. See also, Judge Pettiti's judgment in *Malone v UK* (n 195), p 40.
[313] See, for example, *Kennedy v UK* (n 308) para 153; *Leander v Sweden* (n 229) para 60. Siofra O'Leary also argues that this approach is taken by the ECtHR when determining the margin of appreciation in surveillance cases in, 'Balancing rights in a digital age' (2018) Irish Jurist 59 (discussed in section 3.3, below).
[314] Stavros Tsakyrakis, 'Proportionality: An assault on human rights?' (2009) 7 International Journal of Constitutional Law 468, 483; Blanca Ruiz, 'Privacy in telecommunications: A European and an American Approach' (The Hague: Kluwer Law International, 1996) 181.
[315] Tsakyrakis ibid 483.
[316] Chan (n 310) 1.

ECtHR took a much more structured and rigorous approach to the application of the proportionality principle than can be seen elsewhere in its surveillance case law.[317]

3.2.1.1 S and Marper v UK: an example of proportionality strictu sensu

In *S and Marper v UK*, the ECtHR progressed through its application of the proportionality test as follows: first, it confirmed the legitimacy of the scheme, accepting that the retention of DNA profiles, cellular samples and fingerprints was for crime prevention; second, it established the necessity of the regime, concluding that there were advantages to having comprehensive databases of the concerned data as it contributed to the detection and prevention of crime; third, it considered the suitability of the regime, at which point it raised concerns over the fact that the UK (excluding Scotland) was the only Council of Europe state to permanently store the DNA of persons who had not been convicted of a crime.[318] This led the Court to consider whether there existed 'relevant and sufficient reasons' behind the restriction.[319]

Whilst the UK government argued that the retention of the data was indispensable in the fight against crime,[320] the ECtHR took the noteworthy step of engaging with statistical evidence from both sides of the case – a step it had only previously taken under the legality requirement.[321] In doing so, the Court found that the successful DNA matches could have 'been made in the absence of the present scheme' and that there thus existed less restrictive ways in which to achieve the same goal.[322]

Finally, it considered whether the retention struck a 'fair balance between competing public and private interests,' in other words, the *proportionality strictu sensu* branch of the test.[323] In carrying out this final stage of its proportionality analysis, the Court considered the consequences of 'blanket and indiscriminate' retention of the material,

---

[317] *S and Marper v UK* (n 235) para 50.
[318] Ibid paras 105; 109-110; 117.
[319] Ibid para 114.
[320] Ibid para 115.
[321] Ibid paras 115-117. See, *Association for European Integration and Human Rights and Ekimdshiev v Bulgaria* App no. 62540/00 (ECtHR, 28 June 2007), para 92; and, *Iordachi v Moldova* (206), para 52.
[322] *S and Marper v UK* (n 235) para 116.
[323] Ibid para 118.

in particular: its impact on the private life of individuals whose information was stored (especially minors); the risk of increased stigmatisation; and, the negative impact on societal interests, such as the presumption of innocence.[324] It subsequently concluded that a fair balance had not been struck and the regime disproportionately interfered with Article 8(1).[325]

It is uncertain why the ECtHR took such a rigorous approach to the proportionality test in *S and Marper*. Perhaps because the retention scheme constituted such a stark deviation from the norm of other states, the Court was enabled to carry out a more in-depth analysis of the scheme's proportionality. The existence of such broad consensus among member states, especially neighbouring Scotland, would have also made this approach less constitutionally stressful than would have been the case if no such consensus existed.[326] The case also presented the Court with an opportunity to provide guidance on the treatment of this particular genre of data. This supports van Dijk and van Hoof's description of proportionality as a 'feedback mechanism' implemented in cases for which the application of precedent would not be possible or yield an appropriate answer.[327]

Notwithstanding the reasons behind the ECtHR's approach, *S and Marper* shows that greater substantive reasoning can be carried out via a fuller application of the proportionality test than via the more pragmatic approach of the 'in accordance with law' requirement. Whilst the latter can 'offer[s] a level of concreteness and consistency,'[328] *S and Marper* shows that the former provides more scope to the judiciary to provide meaningful insight and guidance on how a fair balance might be struck between individuals' private life and the societal need for surveillance. Scope for this level of engagement with the proportionality test is important to recognise within the contemporary surveillance landscape where new types of data are

[324] Ibid paras 122, 124.
[325] Ibid para 125.
[326] Murphy (n 275) 516.
[327] Van Dijk et al (n 311) 604.
[328] Maria Helen Murphy, 'The relationship between the European Court of Human Rights and national legislative bodies: Considering the merits and risks of the approach of the Court in surveillance cases' (2013) 3 Irish Journal of Legal Studies 65,76.

increasingly being swept up by mass surveillance regimes. As will be shown in Chapter 5's analysis of the IP Act, the proportionality of these practices is highly contentious and hotly debated. Thus, guidance from the ECtHR would be especially useful. Chan warns that, failing to do so risks losing 'the protective force expected of rights review'[329] and reducing the 'rigour of scrutiny to a level below what is appropriate for human rights cases.'[330] In saying this, the Court must not be so rigorous in its approach to proportionality that it unduly restricts the state's enjoyment of the margin of appreciation.

3.3 Margin of appreciation

The margin of appreciation refers to the scope of deference awarded to contracting states in balancing the need to pursue a legitimate aim and interfering with a convention right. In this sense, it can be described as a 'grant of "breathing space" to national authorities.'[331] The origins of the doctrine have been traced back to concepts of deference in domestic public law where, when influenced by factors outwith the bounds of their own institutional competence, judges may refrain from interfering with decisions of other government branches (unless warranted by the circumstances).[332]

Like the principle of proportionality, there is no explicit reference to the margin of appreciation in the ECHR. However, the doctrine plays an important role, working as a 'lubricant in the working of the Convention' by enabling the ECtHR to develop European-wide rights standards whilst simultaneously respecting the diversity of circumstances across Contracting States.[333]

Typically, in surveillance cases where states seek to justify interferences with Article 8(1) on national security or prevention of crime grounds, a wide margin of appreciation has been granted by the ECtHR. As covered above, in *Klass* it was held that, 'as

[329] Murphy ibid 9.
[330] Ibid 11-12.
[331] Howard Charles Yourow, 'The margin of appreciation doctrine in the dynamics of European human rights jurisprudence' (1987) 3 Connecticut Journal of International Law 111, 118
[332] Andrew Legg, The margin of appreciation in international human rights law (Oxford, 2012) 1-2.
[333] Ronald Macdonald, 'The margin of appreciation' in Ronald Macdonald et al (eds) *The European system for the protection of human rights* (Nijhoff, 1993) 83 and 122.

concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion,' and it is not for the Court to substitute its own assessment for that of the national authorities.[334] However, the ECtHR went on to note that the state does not enjoy an unlimited discretion to subject persons to secret surveillance in the name of espionage and terrorism.[335] Consequently, it placed emphasis on the adequacy and effectiveness of the law's safeguards.[336] The ECtHR thus focusses on guarantees and safeguards provided by domestic laws and considers the purpose behind the surveillance regime at issue (such as, defending national security against espionage and terrorism in *Klass*).[337] This approach can also be seen in many of the other cases examined in this chapter, including: *Zakharov*;[338] *Leander*;[339] *Kennedy*;[340] and, *Szabo and Vissy.*[341]

However, such a wide margin of appreciation is not always granted by the Court. For example, in *S and Marper v UK* it was held that

> 'the margin will tend to be narrower where the right at stake is crucial to the individuals' effective enjoyment of intimate or key rights. Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the state will be restricted.'[342]

Consequently, the 'intrinsically private character' of the material concerned in *S and Marper* led the ECtHR to restrict the margin of appreciation and exercise a more rigorous scrutiny of the regime (discussed above).[343] The gradations of an intrusion will thus serve to influence the margin of appreciation awarded to national

[334] *Klass v Germany* (n 199) para 49.
[335] Ibid.
[336] Ibid para 50.
[337] Siofra O'Leary (n 313) 88.
[338] *Zakharov v Russia* (n 204) para 232.
[339] *Leander v Sweden* (n 229) para 59.
[340] *Kennedy v UK* (n 308) para 154.
[341] Szabo and Vissy v Hungary (n 266) para 57.
[342] *S and Marper v UK* (n 235) para 102.
[343] Ibid para 104.

authorities.[344] This approach has been fairly effective until now, however, as shown in the following chapters, this approach is under increasing duress in the Big Data era where relatively insensitive communications data are swept up under mass state surveillance regimes. Upon aggregation and analysis, such data can become even more revelatory than the content of a communication, exposing various patterns and aspects about one's private life. For these reasons, the CJEU's approach to the determination of discretion might be more suitable for the current landscape.

3.3.1 Determining discretion: ECtHR vs CJEU

The approach taken by the ECtHR towards the margin of appreciation in surveillance cases differs from that taken by the CJEU. The latter has shown a willingness to restrict the area of discretion awarded to states and the EU legislature within its recent surveillance jurisprudence. This is particularly evident in the *Digital Rights Ireland* ('*DRI*') case where it held that the Data Retention Directive 2006/24 enabling the mass collection and retention of communications data constituted a disproportionate interference with the rights to private life and data protection under the EU Charter.[345] In reaching this conclusion, the CJEU severely circumscribed the EU legislature's discretion

> 'in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24.'[346]

Thus, the CJEU restricted the legislature's margin of appreciation on the basis that vast quantities of data were being gathered and retained, as opposed to being based on the sensitivity of the data.[347]

---

[344] O'Leary (n 313) 88.
[345] *DRI* (n 15).
[346] Ibid para 48.
[347] O'Leary (n 313) 88.

The difference between the ECtHR and CJEU's approach is relevant to this thesis because the latter potentially affords greater protection to privacy in the contemporary surveillance landscape. As will be demonstrated in Chapters 3 and 4, surveillance is increasingly geared towards the mass collection, retention and automated processing of individuals' communications data in the digital age. Whilst this data is not necessarily overly intrusive or personal on its own, when aggregated into vast databases and automatically processed, it can be highly revelatory about one's life. Under the ECtHR's approach, a wide margin of appreciation may still be granted to states in relation to the necessity of such mass surveillance regimes on the basis that the data collected is not overly sensitive. However, under the CJEU's approach, a more restricted margin of appreciation is granted, as seen in *DRI*.

4 Group privacy

With the growth of Big Data and bulk surveillance which target everyone as opposed to just 'someone,' it is necessary to consider the scope for group privacy under Article 8. The sufficiency of this scope will be examined in Chapter 4 in light of the contemporary surveillance landscape illustrated in Chapter 3.

4.1 Defining the group

Article 34 of the ECHR states:

> 'The Court may receive applications from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto. The High Contracting parties undertake not to hinder in any way the effective exercise of this right.'

The Convention thus allows states, natural persons, legal persons, and groups of individuals to submit a complaint to the ECtHR.[348] Whilst it would appear that groups

[348] Article 33 of the ECHR also enables states to submit an inter-state complaint to the ECtHR.

are thus protected under Article 8, it is actually unclear how and in what circumstances a group might successfully submit a claim to the ECtHR.

By virtue of Article 34, the ECtHR will not typically accept *actio popularis* claims (claims brought by a claimant(/s) on behalf of others or general society) which requires the claimant(/s) to be the victim(/s) of the alleged violation. This implies that claims of groups acting on behalf of a general or societal interest would not be permissible under the ECHR. However, groups of individuals who have each suffered the same harm are capable of bundling their claims together and so, in this sense, a group privacy right might be said to exist.[349] In a surveillance context, this would enable a group of individuals whose Article 8 right had been interfered with by a particular surveillance measure to submit their claims together. For example, in *Petri Sallinen and others v Finland*, the search and seizure of material from the first applicant's law office, was held to interfere with both his and his clients' Article 8 right.[350] However, Bart van der Sloot argues that this is really just an aggregation of individual claims seeking to protect their own individual interests rather than an autonomous group privacy right.[351]

4.2 Scope for group privacy

In light of van der Sloot's argument above, it is argued that the need for a shared individual interest prohibits an autonomous group privacy right from being enjoyed under Article 8. This is potentially problematic in the Big Data era where data is no longer just gathered about a specific person for a particular purpose, but rather, on an unspecified number of people who are often unaware of their data being gathered (see Chapters 3 and 4). Consequently, it is increasingly difficult for individuals to substantiate a concrete, personal harm arising from the bulk gathering of their data. Rather, this type of mass surveillance poses

---

[349] See for example, *Maldovan and others v Romania (no.2)* App nos. 41138/98 and 64320/01 (ECtHR, 12 July 2005).
[350] *Petri Sallinen and others v Finland* App nos. 50882/99 (ECtHR, 27 September 2009).
[351] This conclusion is also reached by Bart van der Sloot in 'Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under Article 8 ECHR' in Taylor et al (n 61) 211-215.

> 'more of a general concern as they undermine the trust people have in governmental institutions and perhaps more importantly, undermine the minimum conditions for the legitimate use of power.'[352]

However, the law's focus on individual interests may mean that claims against the more general, societal harms posed by these regimes are not possible. This reflects the concerns of Bennett and Raab in their examination of the conventional privacy paradigm.[353] Van der Sloot, consequently, argues that this has created 'a big chasm between the technological developments and the juridical paradigm.'[354]

However, van der Sloot locates a potential solution to this problem via the development of the ECtHR's approach in *Klass* where it held that those at risk of surveillance could be considered a 'victim' for the purposes of engaging Article 8(1) (see section 1.1.2 above). This could, therefore, enable Big Data surveillance to be challenged on a group level given that victimhood is created by the risk of surveillance practices as opposed to a specific, personal harm having to be substantiated by the individual(s). Should it be accepted that *Klass* creates scope for a group privacy right to be enjoyed under Article 8, the ECtHR need only develop the 'mere existence' test so that it is applied more consistently.[355]

However, it is questionable whether this would necessarily constitute a 'group' privacy right on the basis that it does not really enable a group to develop its identity and promote their interests as a 'group' in the traditional sense.[356] In agreement, van der Sloot argues that there are only two ways to create a real group privacy right: (i) change the fundamental basis of the human rights and legal framework that is based on the individual; and, (ii) acknowledge that 'to accept group privacy is to move beyond the

---

[352] Ibid 217.
[353] See Introduction, section 2.3.
[354] Van der Sloot (n 351), 216. Similar conclusions also reached in Alessandro Mantelero, 'From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era,' and Luciano Floridi, 'Group privacy: a defence and an interpretation,' in Taylor et al (n 61).
[355] This was van der Sloot's conclusion in van der Sloot (2015) (n 209).
[356] Van der Sloot (n 351) at fn 27. This conclusion constituted a development of his previous argument in van der Sloot (n 209) which focussed on the development of the 'mere existence' test by the ECtHR.

legal realm' and, therefore, incorporate ethical and political perspectives.[357] These recommendations are not mutually exclusive, rather they should be viewed as necessary steps towards realising a comprehensive group privacy right in the Big Data era.[358]

The impact of such a restricted scope for a real 'group' privacy right under Article 8 of the ECHR on the protection of privacy in the digital age is demonstrated in Chapter 4 via an analysis of the bulk, data-focussed powers introduced by the IP Act. Chapter 6 considers ways in which group privacy might be better protected within the contemporary surveillance landscape. Whilst this thesis agrees with van der Sloot's conclusion that group privacy issues require a progression beyond the legal domain, due to the restricted scope of this thesis, the discussion in Chapter 6 focusses on ways in which the legal approach to group privacy might be improved.

5 Conclusion

This chapter has served a definitional purpose, exploring the meaning of privacy under Article 8 of the ECHR. This enables the impact of the IP Act's approach to the contemporary surveillance landscape to be critically assessed in terms of its impact on privacy in Chapter 5. The following summarises the main conclusions of this chapter and their relevance to subsequent discussion.

This chapter has shown that the ECtHR adopts a wide definition of 'private life' which provides a broad platform for claims against surveillance to be made. For example, the 'mere existence' of surveillance legislation that causes the individual to alter her behaviour can constitute harm in the eyes of the Court and can establish victimhood for the purposes of engaging Article 8(1). In addition, expectations of privacy can persist outwith traditionally private spaces, such as in public streets (*Peck*) or over public information (*Rotaru*).

[357] Van der Sloot (n 351) 223.
[358] Ibid.

As will be demonstrated in Chapter 3, the ECtHR's wide-ranging notions of private life, harm, victimhood, and expectations of privacy are particularly important within the contemporary surveillance landscape where the digitalisation of society has created new types of data and opportunities for surveillance that challenge traditional notions of privacy. The ECtHR's flexible approach helps to ensure that new genres of information are not excluded from the scope of Article 8(1) which, in turn, is capable of offering protection to even the most public types of information, even when shared or published by the individual.

However, this protection is limited by the ECtHR's emphasis on the gradations of an intrusion (or layering of information) when determining the legality, necessity, and proportionality of an interference under Article 8(2). This was shown via a comparison between the ECtHR and CJEU's approach to determining discretion. It was argued that the ECtHR's approach is becoming less suitable in the Big Data era where the surveillance of communications data will not always be sufficient to trigger the Court's application of stricter safeguards or its restriction of discretion awarded to national authorities. As a result, contemporary surveillance practices that pose serious threats to privacy, such as the mass surveillance of communications data, may not be as strictly regulated as they should be. This will be demonstrated further in Chapter 5 via an examination of the extent to which Article 8 corrects the IP Act's approach to key characteristics of the contemporary surveillance landscape posing a risk to privacy.

Chapter 3 The contemporary surveillance landscape

Introduction

This chapter illustrates the contemporary surveillance landscape and identifies three legal implications emerging from it: (i) the collapse of traditional dichotomies; (ii) the participation of the individual; (iii) an increased need for group privacy. It is argued that the law must respond to these implications in order to preserve privacy in the digital age. The extent to which this is achieved by the IP Act is examined in the following chapter.

This chapter is structured into two parts: (i) waves of surveillance theory; and, (ii) sites of third wave surveillance. Part 1 provides a theoretical overview of surveillance as means of identifying and illustrating characteristics of the contemporary surveillance landscape. Galic et al structure surveillance theory into three roughly chronological 'phases' as follows: (i) the panopticon and panopticism; (ii) post-panoptical theories; and, (iii) contemporary conceptions.[359] This structure is adopted for Part 1, although the notion of 'waves' of surveillance are used instead of 'phases.' This imagery is preferred as it highlights the roughly chronological structure of the surveillance theories and the overlaps between them, with each being formed in response to or on the basis of its predecessor. Part 1 focusses predominantly on the third and final wave which is representative of the current surveillance landscape. The theoretical foundation of this chapter helps to bridge the chasm between surveillance studies and legal scholarship described by Cohen and discussed in the Introduction to this thesis.[360] Part 2 goes on to examine social media and smartphones as 'sites of third wave surveillance.' These examples serve to illustrate the reality of the third wave surveillance landscape and the legal implications that flow from it. These 'sites' are

[359] Galic et al, 'Bentham, Deleuze and beyond' (n 64). Instead of 'phases,' the authors refer to 'stages' of surveillance theory in Galic et al, 'Surveillance theory and its implications for law' (n 64).
[360] Cohen (n 3).

particularly helpful in demonstrating the active participation of the individual in the contemporary surveillance landscape and the benefits that flow from this.

By illustrating the benefits of surveillance brought about by the participatory turn in surveillance, this thesis is able to argue that the law's acknowledgment of the role of the individual as both an object and source of surveillance is important not only for the preservation of privacy in the digital age, but also for the protection of benefits bestowed on civil society by the contemporary surveillance landscape.

Part 1 Waves of surveillance theory

This part illustrates the contemporary surveillance landscape by providing a theoretical overview of surveillance. As acknowledged in the Introduction to this thesis, surveillance studies scholarship is superior to legal scholarship in its unpacking of surveillance practices, establishing emerging cultures and themes to question, diversify and refine traditional conceptions of surveillance. This part is therefore structured according to three 'waves' of surveillance theory to illustrate the technological and cultural changes that the contemporary surveillance landscape has undergone. The UK's approach to these changes can subsequently be established in Chapter 4.

The first wave of surveillance covers the theories of Jeremy Bentham and Michel Foucault on the panopticon and panopticism, respectively.[361] First wave surveillance is architectural, disciplinary, and hierarchical with central institutions watching over subjects. Key to the first phase is the internalisation of the whips within the subjects of surveillance. The second wave is more infrastructural, less physical, and more controlling than disciplinary in nature. In second wave theories, the gaze is less centralised and is spread out to other watchers, namely the corporation. The impact of the digital on surveillance is seen in second wave theories with scholars like Haggerty and Ericson demonstrating the re-direction of the gaze towards persons' data (as opposed to their physical beings) in order to control their access to goods and

[361] Bentham (n 5); Foucault (n 9).

services.[362] Finally, the third wave builds on the first and second wave by extending them to include contemporary practices of surveillance prevalent in the 21st century, such as social sorting, peer-to-peer surveillance, and sousveillance. Third wave theories do not deny that disciplinary and controlling or state and corporate surveillance exists, rather, they acknowledge that these have actually been enhanced in the digital age. However, they also highlight the additional agency of the individual in surveillance who, as a result of the digital revolution, is now able to participate in and use surveillance for entertaining and even empowering purposes. Third wave theories thus recognise the latitude of the gaze in the contemporary surveillance landscape as well as its longitude.

1 First wave surveillance: the panopticon and panopticism

First wave surveillance theories are characterised by the hierarchical watching of the individual by an omnipresent centralised watcher for the purpose of inducing self-discipline within the subject.[363] This notion of disciplinary surveillance was advanced by Foucault in his theory of 'panopticism'[364] which was inspired by Jeremy Bentham's architectural design for a prison – referred to hereafter as the 'prison-panopticon.'[365] The following identifies the main characteristics of these theories which continue to be seen in the current surveillance landscape.

1.1 Bentham's prison-panopticon

Bentham's 'prison-panopticon' was an architectural design for a penitentiary that sought to reform prisoners through surveillance.[366] At the periphery of the structure is an annular building divided into cells and, at the centre, a watchtower where an inspector sits. The inmate can see the watchtower but, through the use of lighting,

[362] Kevin Haggerty and Richard Ericson, 'The surveillant assemblage' (2000) 51 The British Journal of Sociology 605.
[363] Galic et al (n 64).
[364] Foucault (n 9).
[365] Bentham (n 5).
[366] Bentham (n 5). Although, it ought to be noted that Bentham was not the original architect of the structure which was designed by his brother, Samuel Bentham, for use within a Russian factory, see Philip Schofield, *Bentham: a guide for the perplexed* (Continuum, 2009) 72, and Ian Christie, *The Benthams in Russia, 1780-1791* (Oxford, 1993) 177.

cannot know whether the inspector is watching him or not, thus rendering power 'visible and unverifiable' within the structure.[367] Through the use of surveillance, Bentham sought to induce meaningful reform within the inmate and circumvent the use of brutal punishments upon the body which he condemned for being 'preventative legislation' - a mere deterrent to crime as opposed to a way of inducing meaningful reform within the individual.[368]

Bentham's plan for the prison-panopticon, and the panopticons generally, are thus representative of his utilitarian conception of harm. He is considered a classical utilitarian, alongside Mill and Hume, who place pleasure and pain at the centre of their philosophies.[369] Bentham was focussed on the achievement of happiness and pleasure for the greatest number of people and sought to reform 'bad' laws and social practices that went against the grain of this utilitarian ideal, such as those inflicting pain upon the individual (this is referred to as the 'principle of utility'). [370] Bentham thus synonymises 'good' with pleasure and 'bad' with pain. This is supported by Ayer who writes that Bentham believed, 'pleasure is the only good and pain the only evil,' and, 'conceived of "good" as the object of desire and "evil" as the object of aversion.'[371] Under this logic, the use of physical punishments in prisons was harmful as it inflicted pain upon the inmate, and so the use of surveillance within the Panopticon was desirable as it circumvented such harm and, thus, increased happiness.

The above 'Benthamite utilitarianism' has divided academic opinion. For example, the liberal school view Bentham as a promoter of civil and political rights and stress the benefits of the structure for the inmates.[372] One such thinker, Philip Schofield, even hypothesises that Foucault's interpretation of the Panopticon which emphasises the

---

[367] Foucault (n 9) 201.
[368] Andrew Zimmerman, 'Legislating being: The spectacle of words and things in Bentham's panopticon' (2008) 3 The European Legacy 72, 73.
[369] Frederick Rosen, *Classical utilitarianism: from Hume to Mill* (Routledge, 2003) 8.
[370] Jeremy Bentham, 'An introduction to the principles of morals and legislation' in Alan Ryan (ed) *J.S. Mill and Jeremy Bentham: utilitarianism and other essays* (Penguin Books, 2004) 65.
[371] Alfred Jules Ayer, 'The principle of utility' in G W Keeton and G Shwarzenberger (eds) *Jeremy Bentham and the law: a symposium* (Steven & Sons ltd, 1948) 245-248.
[372] HLA Hart, *Essays on Bentham: studies in jurisprudence and political theory* (OUP, 2001); Frederick Rosen, *Jeremy Bentham and representative democracy: a study of the constitutional code* (Oxford Clarendon Press, 1983); Schofield (n 366) 70.

harm caused by an omnipresent gaze (see below) 'would have seemed very odd to Bentham, who regarded his Panopticon prison as humane, and an enormous improvement on the practices of the criminal justice system of the time.'[373] However, the authoritarian school condemn Bentham as a precursor of totalitarianism and the epitome of disciplinary society – a paternalistic writer of control who sought to impose majoritarian approved norms on individuals, against their wishes and at the expense of the minority.[374] However, Brunon-Ernst argues that this latter school of thought has been influenced by Foucault's gross (mis-)interpretation of the Panopticon that constitutes Bentham as a 'forerunner of Big Brother.'[375]

Ultimately, the interpretation of the panopticon depends upon one's conception of 'harm.' For example, Benthamite scholars associate harm with violence and physical pain and so the internalisation of the gaze is a way of avoiding this harm. However, critics of Bentham view the enforcement of irresistible control and suppression of individuality as harmful. Consequently, the internalisation of the gaze comes to be viewed as something akin to self-harm with the subject forsaking their own autonomy to succumb to the will of the watcher. This arguably aligns with the ECtHR's concept of harm in *Klass v Germany*, where the alteration of one's behaviour by the mere existence of surveillance legislation constituted an interference with Article 8(1).[376]

From the above summary, the following key themes and characteristics of the first wave are identified: discipline; prevention and deterrence; omnipresence; and, the internalisation of the gaze. The extent to which one considers the gaze within the Panopticon as harmful ultimately depends upon one's conception of harm. In Bentham's later panopticon designs, privacy is granted in varying degrees. For example, in the pauper panopticon the subjects were allowed to hang blinds to have marital sex. In the chrestomathic (school) panopticon, the students were able to leave

---

[373] Schofield (n 366) 70.
[374] See: Elie Halevy, *The Growth of Philosophic Radicalism* (Martino Fine Books, 2013); Douglas Long, *Bentham on Liberty: Jeremy Bentham's idea of liberty in relation to his utilitarianism* (University of Toronto Press, 1977); Gertrude Himmelfarb, *Victorian Minds* (Weidenfield and Nicolson, 1968).
[375] Anne Brunon-Ernst (ed) *Beyond Foucault: new perspectives on Bentham's panopticon* (Ashgate Publishing, 2013) 3.
[376] *Klass v Germany* (n 199) paras 33-34. See Chapter 2, section 1.1.2.

the structure thus limiting the gaze of the teacher to school hours. Similarly, in his fourth and final design of the 'constitutional panopticon,' the gaze was to be exerted by the many (citizens) upon the few (government ministers).[377]

It could, subsequently, be argued that the absence of any privacy in the prison-panopticon is not viewed as harmful by Bentham on the basis that convicts sacrifice any right to privacy upon the committal of crime and thus have no expectation of privacy in the first place. Clearly, this concept of harm (and privacy) does not fit within the current human rights framework where such rights are not luxuries to be revoked upon bad behaviour. Therefore, this thesis endorses the ECtHR's approach in *Klass* and views the internalisation of the gaze as harmful in so far as it unjustifiably interferes with Article 8(1). This is supported by the following discussion of Foucault's panopticism which emphasises the harm caused by an omnipresent gaze.

1.2 Foucault's panopticism

In the 1970s, Foucault used the panopticon to demarcate a shift from sovereign to disciplinary power, arguing that 'panopticism is the general principle of a new 'political anatomy' whose object and end are not the relations of sovereignty but the relations of discipline.'[378] Foucault extended the architecture of the prison-panopticon to other areas of society - such as the school, the military, the hospital, and the factory - in order to demonstrate the existence of a disciplinary society in which everyone is capable of being subjected to surveillance. Thus, for Foucault the Panopticon was emblematic of a disciplinary power running through society that affects, 'the grain of individuals, touches their bodies and inserts itself into their actions and attitudes, their

---

[377] For discussion of Bentham's chrestomathic and constitutional panopticons see Anne Brunon-Ernst, 'Deconstructing panopticism into the plural panopticons' in Anne Brunon-Ernst (n 375). Some have consequently argued that Bentham also influenced Foucault's later work on 'governmentality' and not just his theory of panopticism. 'Governmentality' refers to the techniques and mechanisms by which government governs – also referred to as 'the art of government' (see: Michel Foucault, *The birth of biopolitics: lectures at the College de France 1978-79* (Palgrave Macmillan, 2008); Michel Foucault, 'The subject and Power' in *Power: volume 3* (Penguin, 2002)). For example, Laval argues that, 'one needs to go beyond "Discipline and Punish" to grasp the importance Bentham had for Foucault' in Christian Laval, 'From discipline and punish to the birth of biopolitics' in Brunon-Ernst (n 375) 59. See also, Brunon-Ernst (n 375) 39.

[378] Foucault (n 9) 208.

discourses, learning processes and everyday lives.'[379] Similar to the prison-panopticon, Foucault's panopticism strived towards the creation and installation of norms of behaviour in the individual. He refers to this process as 'normation' which makes it possible to measure individuals' according to their conformity with the norm as well making it easier to identify the non-conformer.[380] Thus, Foucault developed Bentham's panopticon beyond a simple design in architecture to a theorisation of governance in Western society by shifting 'the perspective from the *goal* of governing to the *mode* of governing.'[381]

Similar to the prison-panopticon, prevention, discipline, and hierarchy all remain as key characteristics of Foucault's panopticism. These forms of disciplinary surveillance remain visible in the current landscape and have been attributed to different types of electronic surveillance.[382] In fact, there has been renewed interest in the Panopticon and panopticism (particularly in the popular press) in the post-Snowden climate where the omnipresent and hierarchical gaze of the state is particularly pronounced.[383] However, as shown below, we have now progressed beyond Foucault's disciplinary society with the gaze taking on more functions and being carried out by actors beyond the state, such as the individual. Technology has played a large part in this development with Foucault himself noting the likelihood of a 'control society' where surveillance is exercised more informally (see section 2 below). Some have also argued that Bentham himself progressed beyond the disciplinary society in his later panoptic writings, as shown by the aforementioned school and constitutional panopticons where the gaze was more restricted.

---

[379] Michel Foucault, *Power/Knowledge: selected interviews and other writings 1972-1977* (ed C Gordon) (Pantheon Books, 1980) 39.
[380] Foucault (n 9) 57.
[381] Foucault (n 9). Foucault's focus on the 'mode' of governing was developed in his later work on 'governmentality,' see Foucault (n 377).
[382] Galic et al, 'Surveillance theory and its implications for law' (n 64) 735.
[383] See, for example, Julian Sanchez, 'Snowden just showed us how big the panopticon really was. Now it's up to us' (*Guardian news*, 5 June 2014) <https://www.theguardian.com/commentisfree/2014/jun/05/edward-snowden-one-year-surveillance-debate-begins-future-privacy> accessed 20 June 2018.

1.3 Summary

Based on Bentham's prison-panopticon and Foucault's panopticism, and in accordance with Galic et al, the characteristics of first wave surveillance can be summarised as follows: (i) physical and visible; (ii) state-oriented; (iii) focussed on the bodies of the underclass; (iv) disciplinary; and, (v) negative.[384] However, as indicated by the later works of Bentham and Foucault, and as shown in the following sections, society has progressed beyond the disciplinary function of the gaze which, although relevant, is no longer the only gaze in operation across the contemporary surveillance landscape.

2 Second wave surveillance: post-panoptical theories

Second wave surveillance theories emerged in response to 'the rise of (consumer) capitalism as a global political system' in the late 1970s.[385] Accompanying this development were technological advancements, in particular the computer and the database, which enabled non-state actors to gather, retain and process an increasing volume of data generated by individuals. These developments led scholars away from first wave theories which were criticised for being unidirectional and static, and encouraged the development of alternative theories to illustrate the shift from a disciplinary society to a society of control. The following establishes the main characteristics of second wave surveillance via an analysis of Haggerty and Ericson's 'surveillant assemblage.'[386] Although other second wave surveillance theories are discussed by Galic et al,[387] the 'surveillant assemblage' is the main focus here due to its standing as a 'conceptual benchmark' in post-panoptical literature.[388]

---

[384] Galic et al, 'Surveillance theory and its implications for law' (n 64), 735.
[385] Galic et al (2017) (n 64), 736.
[386] Kevin Haggerty and Richard Ericson (n 362).
[387] Including: Gilles Deleuze, 'Postscript on societies of control' (1992) 59 October 3; Shoshana Zuboff, 'Big other: surveillance capitalism and the prospects of an information civilisation' (2015) 30 Journal of Information Technology 75.
[388] Sean Hier, 'Probing the surveillant assemblage: on the dialectics of surveillance practices as processes of social control' (2003) 3 Surveillance & Society 399, 400.

2.1 The surveillant assemblage

Haggerty and Ericson developed the 'surveillant assemblage' as an alternative theory to Foucault's panopticism and Orwell's *Nineteen Eighty-Four* which heretofore had provided the dominant metaphors for understanding contemporary surveillance.[389] They criticise both works for conceptualising surveillance as a mechanism of repression and discipline that is only exercised by the state. They especially criticise Foucault for failing to acknowledge developments in technology that 'transformed the hierarchies of observation.'[390] In turn, they proposed a new theory of surveillance inspired by Guattari and Deleuze's work on 'assemblages' to depict the increasing convergence of surveillance technologies.[391]

Deleuze and Guattari's 'assemblage' can be described as a 'multiplicity of heterogeneous objects, whose unity comes solely from the fact that these items function together, that they "work" together as a functional entity.'[392] Within these assemblages, are 'discrete flows of an essentially limitless range of other phenomena such as people, signs, chemicals, knowledge and institutions.'[393] Haggerty and Ericson invoke this concept of the assemblage to capture the increasing convergence of once discrete surveillance practices - a convergence driven by 'the desire to bring systems together, to combine practices and technologies and integrate them into a larger whole.'[394] To illustrate this theme of convergence, they give the example of electronic monitoring, or 'tagging,' which has been developed to comprise a host of different surveillance techniques (such as remote alcohol testing, voice radio, and programmed contact technologies) for the tracking of offenders.[395] The 'surveillant assemblage' thus refers to the combination of previously disparate surveillance practices into a single functioning entity in order to capture previously discrete flows of information

---

[389] Orwell (n 5).
[390] Haggerty and Ericson (n 383) 617.
[391] Gilles Deleuze and Felix Guattari, *A Thousand Plateaus*: *capitalism and schizophrenia* (Minnesota Press, 1987).
[392] Paul Patton, 'Metamorphologic: bodies and powers in a thousand plateaus' (1994) 25 Journal of the British Society for Phenomenology 157, 158.
[393] Haggerty and Ericson (n 362) 608.
[394] Ibid 610.
[395] Ibid.

that would otherwise remain unknowable and unrecordable. Technology is positioned as playing an integral role in facilitating this convergence.

2.1.1 The 'data double'

A main characteristic of the surveillant assemblage is the decorporealisation of the human body into a 'data double.'[396] Haggerty and Ericson argue that in the digital age, the body has become a

> 'flesh-technology hybrid' through processes of tagging and the reconstruction of persons' likes, habits, and lifestyle from 'trails of information which have become the detritus of contemporary life' (also referred to as the 'data exhaust').[397]

The surveillant assemblage is geared toward capturing the flows of this cyborg flesh-technology hybrid in order to produce a 'pure information' version of the individual that is more mobile and amenable to comparison than the physical body.[398] Once the body has been re-constitutionalised into this 'data double,' it can then be 'reassembled and scrutinised' within 'centres of calculation,' such as laboratories, financial institutions, corporate and state headquarters.[399] Data doubles can subsequently form the basis of discriminations by authorising or denying access to goods, services, and power.[400] Therefore, the primary function of the surveillant assemblage can be considered the abstraction of a data double from the individual for subsequent redirection back to the body for the purposes of governance, profit, control, security, or discipline.[401] As an aside, Haggerty and Ericson also note the voyeuristic and entertaining value of surveillance as a driver behind its expansion, with television

---

[396] Ibid 611.
[397] They give the example of the 'HUGS' tag which is an electronic bracelet for infants in order to track their whereabouts (n 362) 611-612.
[398] Ibid 613 and 614.
[399] Ibid 613.
[400] Ibid.
[401] Hier (n 388) 402.

programmes devoted to the airing of CCTV clips, such as 'America's dumbest criminals.'[402]

2.1.2 Rhizomatic surveillance

Again borrowing from Deleuze and Guattari, Haggerty and Ericson describe the surveillant assemblage as 'rhizomatic.'[403] Rhizomes are plants which grow in surface extensions through interconnected vertical root systems. They 'grow like weeds' and, if broken in one spot, can sprout up on either an old or new line.[404] Haggerty and Ericson use the rhizome as a metaphor to illustrate two attributes of the surveillant assemblage: (i) its expansion across society, and (ii) its flattening of surveillance hierarchies.[405] They argue that, like rhizomes which operate through 'variation, expansion, conquest, capture, offshoots,' the gaze has expanded through the development of new surveillance technologies and the convergence of monitoring devices; enabling more of the population to be surveilled.[406] Thus, in comparison with the scope of surveillance in the Panopticon where only select pockets of the population are targeted (such as the incarcerated), in the surveillant assemblage there is an amorphousness of the subject that causes the gaze to shed the physical boundaries of the institution and creep horizontally into the lives of the masses – lives which are 'undulatory, in orbit, in a continuous network.'[407]

Haggerty and Ericson argue that the rhizomatic spread of surveillance transforms pre-existing hierarchies of surveillance.[408] Compared to panoptic theorisations of surveillance where the few see the many, the rhizomatic surveillant assemblage 'allows for the scrutiny of the powerful by both institutions and the general population.'[409] Invoking Mathieson's 'synopticism' where the many see the few, the authors argue that technological advancements coupled with greater accessibility to

---

[402] Haggerty and Ericson (n 362) 616.
[403] Deleuze and Guattari (n 391) 21.
[404] Ibid 9.
[405] Haggerty and Ericson (n 362) 614.
[406] Ibid 614-615; Deleuze and Guattari (n 491) 21.
[407] Deleuze (n 491) 6.
[408] Haggerty and Ericson (n 362) 617.
[409] Ibid.

these technologies have served to partially democratise surveillance.[410] They give the example of the handheld video camera that allows the individual to record police behaviour, and thus, to return the gaze.[411] They subsequently conclude that there now exists a 'rhizomatic criss-crossing of the gaze such that no major population groups stand irrefutably above or outside of the surveillant assemblage.'[412]

2.1.3 Summary

By tearing 'down the walls of the panopticon,' Haggerty and Ericson illustrate the interconnectedness, multi-functionality, and changing hierarchies of surveillance in (consumer) capitalist society.[413] Through the rhizomatic structure of the assemblage, the authors highlight the diminishment of space for disappearance, or what they call 'the disappearance of disappearance.'[414] As argued in the Introduction and will be further illustrated below, this is a feature which has become significantly more pronounced in the digital age with the nascent use of ICTs like social media and smart technologies that enable a persistent tracking of one's location and actions. In this respect, the surveillant assemblage remains highly relevant to modern surveillance society (demonstrating the overlapping of the second and third waves). However, the extent to which the gaze of the assemblage remains a fairly negative and elite-dominated structure with little space for its 'hapless victims…to contain, thwart or even annul it,' fails to recognise the democratisation of surveillance and its use for more entertaining purposes.[415] This shortcoming has led to the development of a third and final wave of surveillance theory with authors highlighting the additional entertaining and empowering uses of surveillance by the individual.

---

[410] Thomas Mathieson, 'The viewer society: Michael Foucault's "panopticon revisited"' (1997) 1 Theoretical Criminology 215.
[411] Haggerty and Ericson (n 362) 618; 'partially democratised' because ultimately the powerful remain more in control of surveillance than the non-powerful and are only subjected to intense forms of scrutiny when circumstances activate the need for it. They give the example of the OJ Simpson case where the murder of his wife led to intense scrutiny of his movements and behaviour.
[412] Ibid.
[413] Kevin Haggerty, 'Tear down the walls: on demolishing the panopticon' in David Lyon *Theorizing surveillance: the panopticon and beyond* (Wilan Publishing, 2006), 23.
[414] Haggerty and Ericson (n 362) 619.
[415] Lyon, *Surveillance studies: an overview* (n 67) 92; Hier (n 388).

3 Third wave surveillance: contemporary conceptions

'As well as the surveillance state and surveillance society, we now have to take account of surveillance culture. Surveillance is not just practised *on* us, we participate *in* it.'[416] Lyon describes this as a recent development that has been brought about by online social networking and handheld smart devices which enable the individual to participate in surveillance for the purposes of 'freedom and fun.'[417] Lyon's argument is reflective of the third wave as it acknowledges the participatory turn in surveillance and its additional functions of entertainment, sociality, and empowerment. Whilst these features of the contemporary surveillance landscape challenge disciplinary and controlling theories, they do not replace them. Rather, the third wave builds on and branches out from the first and second waves in order to capture contemporary surveillance phenomena.[418] The reason for this is that

> 'the increase in size and complexity of surveillance practice seems to make it impossible to develop an over-arching theory of surveillance as a largely unitary concept or phenomenon, as in Foucault's or Deleuze's theories.'[419]

Galic et al thus list the following concepts as the most notable contemporary theories of the third wave: (i) alternative opticons; (ii) sousveillance, and; (iii) participatory surveillance.[420] An overview of each is provided below and subsequently illustrated in Part 2's analysis of smartphones and social media as 'sites of third wave surveillance.'

3.1 Alternative opticons

Numerous iterations of the panopticon have been developed by surveillance theorists to demonstrate the existence of panoptic principles in the current landscape, including:

---

[416] Lyon, *Surveillance after Snowden* (n 1) 3.
[417] Ibid 3-4.
[418] Galic et al, 'Surveillance theory and its implications for law' (n 64) 738.
[419] Galic et al, 'Bentham, Deleuze and beyond' (n 64) 26.
[420] These headings are a mixture of those used by Galic et al (n 64).

the superpanopticon;[421] the participatory panopticon;[422] the synopticon;[423] the panopticommodity;[424] the oligopticon;[425] and, the ban-opticon.[426] Each theory develops the panopticon in an attempt to explain contemporary surveillance phenomena and whilst they highlight the limitations of the Panopticon within the current landscape (ergo the need to adjust it), they simultaneously demonstrate its continued utility in conceptualising surveillance. Some of these theories also demonstrate the relevancy of Deleuze and Guattari's work on surveillance as a mechanism of control. Bigo's 'ban-opticon,' for example, illustrates the re-focussing of surveillance on the control of access in the post-9/11 climate as opposed to the inducement of self-discipline.[427]

The first wave Foucauldian theory of panopticism has also been increasingly invoked by journalists and commentators in the post-Snowden landscape as means of attacking the surveillance practices of the NSA and GCHQ.[428] However, this trend is countered by surveillance scholars like Viadhyanathan and Garrido who argue that the surveillance practices of these agencies are more discrete than those described by Foucault and can also be resisted by the individual's own surveillance practices (as shown in the following discussion on sousveillance).[429] However, this is disputed by Horowitz who underlines the relevance of Foucault's panopticism to contemporary

---

[421] Mark Poster, *The mode of information: poststructuralism and social context* (University of Chicago Press, 1990).
[422] Lyon, *Surveillance studies: an overview* (n 67).
[423] Mathieson (n 410).
[424] Lyon, *Theorizing surveillance* (n 413) 6.
[425] Bruno Latour, *Reassembling the social: an introduction to actor-network-theory* (OUP, 2005).
[426] Didier Bigo, 'Security, exception, ban and surveillance' in Lyon (n 413).
[427] Bigo ibid.
[428] Sanchez (n 383); Sean Gallagher, 'Building a panopticon: the evolution of the NSAs Xkeyscore' (*Arstechnica*, 9 August 2013) <https://arstechnica.com/information-technology/2013/08/building-a-panopticon-the-evolution-of-the-nsas-xkeyscore/> accessed 20 June 2018; John Lancaster, 'The Snowden files: why the British public should be worried about GCHQ' (*Guardian news*, 3 October 2013) <https://www.theguardian.com/world/2013/oct/03/edward-snowden-files-john-lanchester> accessed 20 June 2018. For discussion of commentators' invocation of the Panopticon in the post-Snowden climate refer to Sarah Horowitz, 'Foucault's panopticon: a model for NSA surveillance?' in Miller (n 16) 49-50.
[429] Siva Viadhynathan, 'The rise of the cryptopticon' (2015) 17 Hedgehog Review; Verde Garrido, 'Contesting a biopolitics of information and communications: the importance of truth and surveillance after Snowden' (2015) 13 Surveillance & Society 153.

surveillance trends.[430] For example, she notes Foucault's reconciliation of liberal democratic democracy with the surveillance state which he achieves by showing how steps taken to further our freedom can actually serve to expand state control.[431] This is supported by the following examination of social media as a site of third wave surveillance, individuals subscribe to this ICT for self-serving purposes, such as enhanced sociality, but doing so can simultaneously subject them to (disciplinary or controlling) state and corporate surveillance structures.

The continued relevancy of the Panopticon and panopticism demonstrates the overlapping of the first wave with the third wave. However, the simultaneous inadequacy of these theories to capture the positive features of the contemporary surveillance landscape also highlights the need for new conceptions of surveillance to be developed.

3.2 Sousveillance

Mann et al's theory of 'sousveillance' refers to the 'surveilling of the surveillors' with technology being used to perform acts of counter-surveillance.[432] The potential for sousveillance has grown in the digital era with the proliferation of ICTs like smartphones that make it possible to record, share and scrutinise the watchers. This is evident in Mann's later work where he lists the following as technologies or sites of sousveillance: 'social networking, distributed cloud-based computing, self-sensing, body-worn vision systems, wearable cameras, and ego-centric vision.'[433]

Haggerty also acknowledges sousveillance in his later work on the surveillant assemblage where he argues that the proliferation of surveillance within the digital age enables more people to become viewers, and that viewing others and exposing oneself

---

[430] Horowitz (n 429).
[431] Ibid 51.
[432] Steve Mann, Jason Nolan, Barry Wellman, 'Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments' (2003) 1 Surveillance & Society 331.
[433] Steve Mann, 'The sightfield: visualising computer vision, and seeing its capacity to "See"' Published as part of 2014 Conference on Computer Vision and Pattern Recognition Workshops <https://pdfs.semanticscholar.org/f4f2/f7a1861d667f068f89eccf99793033851c9c.pdf?_ga=2.3916791.678783471.1525191510-1786373483.1525191510> accessed 1 May 2018.

can be liberating.[434] He thus expands the focus of the surveillant assemblage beyond the corporation to reflect the further decentralisation of surveillance and to illustrate other purposes of surveillance brought about by the technological and cultural changes of the contemporary surveillance landscape. Sousveillance is explored in greater depth below via an examination of social media as a site of third wave surveillance that provides citizens with a platform to scrutinise governing bodies from below.

The introduction of the individual as a viewer introduces the third and final theory of the third wave – participatory surveillance.

3.3 Participatory surveillance

Participation has come to be viewed as a 'movement'[435] or 'condition' within the contemporary surveillance landscape where

> 'being involved in doing something and taking part in something with others – has become both environmental (a state of affairs) and normative (a binding principle of right action)…It has become a contextual feature of everyday life in the liberal, capitalist, and technological societies of the contemporary West.'[436]

The theme of 'participation' is particularly prominent in surveillance studies literature where there exists a trajectory of rhetoric on individuals' use of surveillance for the purposes of entertainment, pleasure, and empowerment. This movement has flourished with the arrival of Web 2.0 which refers to internet services and platforms that rely on user-generated content, such as: web blogs, social networking sites (eg Facebook, Twitter, Instagram), and sharing platforms (eg YouTube).[437] The proliferation of these sites has led to various conceptualisations of the individual as a surveillance user

---

[434] Haggerty, 'Tear down the walls' (n 413) 28.
[435] Francesca Bruno refers to the 'participation movement' in 'Surveillance and participation in Web 2.0' in Kirsty Ball, Kevin Haggerty, David Lyon (eds) *Routledge handbook of surveillance studies* (Routledge, 2012) at 345.
[436] Barney et al (n 8) vii.
[437] Bruno (n 435) 344.

capable of monitoring their peers, themselves, and the elite. Thus, as Lyon notes, the spotlight has been turned 'on all our very varied roles in relation to surveillance.'[438]

One of the first theories on the individual as an actor of surveillance was Andrejevic's concept of 'lateral surveillance' which refers to the 'use of tools by individuals, rather than by agents of institutions public or private, to keep track of one another.'[439] Techniques of lateral surveillance could thus include carrying out a Google search on someone or recording them with a smartphone.[440] Andrejevic argues that this is part of a process of responsibilisation of risk whereby, through the democratisation of surveillance technologies, individuals can take on previously centralised duties of monitoring, both of the population and of themselves.[441] Andrejevic's lateral surveillance thus results from state and corporate invitations to become our own protector, 'to become spies – for our own good.'[442] Therefore, instead of transposing pre-existing hierarchies of observation, Andrejevic's 'lateral surveillance' provides something of a supporting infrastructure by characterising lateral surveillance as an extension and amplification of the institutional gaze. However, Andrejevic's failure to demonstrate an awareness of the more positive, empowering, and entertaining exercises of participatory surveillance brought about by Web 2.0 is challenged by Albrechtslund who provides a particularly forthright account of digital social networking as an entertaining and empowering site of surveillance.[443]

Building on Andrejevic's construction of surveillance as mutual, Albrechtslund characterises individuals' data exchange on social media as a form of participatory surveillance.[444] Unlike Andrejevic, Albrechtslund views the mutuality of watching on social media as indicative of a more social and playful side of surveillance, as opposed to individuals being construed as pawns in a dystopian regime of disciplinary

---

[438] Lyon (n 1) 7.
[439] Mark Andrejevic, 'The work of watching one another: lateral surveillance, risk, and governance' (2005) 2 Surveillance & Society 479, 488.
[440] Ibid.
[441] Ibid 489.
[442] Ibid 494.
[443] Albrechtslund (n 8).
[444] Ibid.

surveillance.[445] He argues that contrary to hierarchical conceptions of surveillance where the target is reduced to a hapless victim under the control of the gaze,

> 'social networking and the idea of mutuality…is not about destructing subjectivity or lifeworld. Rather, this surveillance practice can be part of the *building* of subjectivity, and of making sense in the lifeworld.'[446]

Albrechtslund thus conceptualises surveillance on social media as an apparatus for identity formation that enables users to develop relationships, seek out information, and construct their own identity.[447] Albrechtslund does not try to diminish the threats of surveillance online, such as the erosion of privacy, but seeks to promote a more nuanced understanding that captures its 'multi-faceted nature.'[448]

Social media has provided fertile ground for concepts of participatory surveillance, as shown by: Tokunaga's 'interpersonal electronic surveillance;'[449] Lampe et al's 'social searching;'[450] Marwick's 'social surveillance;'[451] and Harcourt's 'expository society' where 'we expose ourselves. We watch others.'[452] In line with Albrechtslund, these theories demonstrate how social media users use surveillance for self-serving purposes like entertainment and sociality. In addition to peer-to-peer surveillance on social media, Marwick and Harcourt also note the self-surveillance practices on these platforms, with users internalising the gaze of their online audience and altering their behaviour and conduct accordingly (for example, by deciding not to share a particular

---

[445] Ibid.
[446] Ibid.
[447] Ibid.
[448] Anders Albrechtslund and Lynsey Dubbeld, 'The plays and arts of surveillance: studying surveillance as entertainment' (2005) 3 Policy Studies 216, 218.
[449] Robert Tokunaga, 'Social networking site or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships' (2011) 27 Computers in human behaviour 705.
[450] Cliff Lampe, Nicole Ellison, and Charles Steinfield, 'A Face (book) in the crowd: Social searching vs. social browsing' (2006) In proceedings of the 2006 20th anniversary conference on computer supported cooperative work 167; Adam Joinson, 'Looking at, looking up or keeping up with people?: Motives and use of Facebook." (2008) in Proceedings of the twenty-sixth annual SIGCHI conference on human factors in computing systems, 1027.
[451] Alice Marwick, 'The public domain: surveillance in everyday life' (2012) 9 Surveillance & Society 378.
[452] Harcourt (n 12) 129.

photograph in case of one's boss, teacher or parent seeing it).[453] Whilst concepts of social media as participatory surveillance will be illustrated below, it suffices to show here the development of a 'user-centred perspective on surveillance' by surveillance studies scholars which adds to, but does not supplant, the top-down, hierarchical focus of the first and second wave theories.[454]

Galic et al argue that the user-centric approach to analysing surveillance has provided a gateway for investigations into the reasons behind individuals' participation in surveillance.[455] For Albrechtslund, individuals participate for entertainment and sociality. Koskela maintains that exhibitionism is empowering for the individual because, 'by revealing their intimate lives, people are liberated from shame and the "need" to hide.'[456] Similarly, Djolakia and Zwick claim that ultra-exhibitionism 'is not a negation of privacy but an attempt to reclaim some control over the externalisation of information.'[457] Exposure is thus construed as a form of counter-surveillance, or 'sousveillance,' in these works.

However, counter-arguments to the empowering and entertaining accounts of participatory surveillance are found in the 'alternative opticons' branch of the third wave where disciplinary and controlling power is located in self-monitoring practices (see section 3.1, above). For example, Whitaker and Lyon's theories of the 'participatory panopticon'[458] and 'panopticommodity'[459] argue (respectively) that panoptic principles at play in the prison have simply moved to 'softer' forms like entertainment and marketing where individuals are seduced into self-disclosure for the purposes of advancing the gaze into new sectors of society.[460] Whitaker gives the examples of ATMs, debit/credit cards, telephone, and online banking which enable

---

[453] Marwick (n 451) 381.
[454] As noted by Galic et al, 'Bentham, Deleuze and beyond' (n 64) 30.
[455] Ibid.
[456] Hille Koskela, 'Webcams, TV shows, and mobile phones: empowering exhibitionism' (2004) 2 Surveillance & Society 199.
[457] Nikhilesh Dholakia and Detlev Zwick, 'Privacy and consumer agency in the information age: between prying profilers and preening webcams' (2001) 1 Journal of Research for Consumers 1.
[458] Lyon, *Theorizing surveillance* (n 413) 6 and 8.
[459] Reginald Whitaker, *The end of privacy: how total surveillance is becoming a reality* (The New Press, 1999) Chapter 6.
[460] Whitaker ibid 141.

convenient, secure, everyday banking, but which simultaneously facilitate the configuration of consumer profiles for targeted marketing (which might still be considered helpful), and on a more sinister level - the identification and exclusion of those deemed 'risky.'[461] Thus whilst participation can be empowering and entertaining, it can also facilitate punishment and control through exclusion.

Furthermore, as noted above, panopticism is increasingly applied to contemporary surveillance practices in the post-Snowden landscape where the NSA's collection of 'Big Data' has led to arguments that the web is being re-centralised.[462] Romele et al note, for example, that social media is now being treated as more of a classical form of Panopticon where, in the words of Foucault, the individual 'is the object of information, never a subject in communication.'[463] However, as noted above, this resurgence of the Panopticon is countered in the literature. Harcourt, for instance, considers the Panopticon to be of limited fit within the 'digital era' as it misses important aspects of contemporary society, particularly the individual's exposure of themselves online driven by a desire to be seen.[464] As such, he argues that, 'we are confronted less with surveillance than with an oligarchical voyeur taking advantage of our exhibitionism.'[465]

Romele at al also argue that 'panopticism is not enough' because it fails to take into account individuals' 'voluntary submission' to surveillance on social media.[466] Borrowing from Etienne de La Boetie, they argue that although individuals are 'forced and cheated' into sharing on these platforms by 'complex strategies' (such as default privacy settings) there is an additional element of 'voluntary servitude.'[467] 'Voluntary servitude' refers to 'an awareness and a positive manner users adhere to the

---

[461] Ibid.
[462] Alberto Romele, Francesco Gallino, Camilla Emmenegger, Daniele Gorgone, 'Panopticism is not enough: social media as technologies of voluntary servitude' (2017) 15 Surveillance & Society 204, 205.
[463] Ibid 207-208.
[464] Harcourt (n 12) 90.
[465] Ibid.
[466] Romele et al (n 462) 135.
[467] Etienne de La Boetie, *The politics of obedience: discourse on voluntary servitude* (First published 1576, Black Rose Books, 1997).

surveillance exercised by and through social media.'[468] In other words, users of social media are aware of the surveillance practices in operation, but continue to participate because they are resigned to the Damoclean sword of surveillance hanging overhead and feel powerless to stop it. In this way, the writers argue that users are 'assuming an active role in their own submission'[469] - which panopticism fails to capture because it 'does not go as far as breaking the direct relationship between awareness and emancipation – a relationship as old as Plato's allegory of the cave.'[470] Although, even post-Snowden, it is questionable just how truly 'aware' we are of the myriad of (discreet) ways in which we are now surveilled in the Big Data era. This is supported by Siva Vaidhyanathan's critique of the panopticon above.[471]

There also exists a Deleuzian, neo-liberal counter-argument to empowering participatory surveillance that argues that the self-tracking facilitated through interactive technologies and social media creates a façade of self-control that, in reality, only enables greater corporate tracking of data doubles for the maximisation of profit and control of access. This is explored by Cohen who examines 'gamification' techniques used within the corporate surveillance context to motivate user participation.[472] She gives the example of high-street retailer 'H&M' which teamed up with an online gaming company to encourage users to come in-store to receive a discount.[473] After exploring the various ways in which participation is used by corporations, Cohen argues that the participatory turn in surveillance has been over-simplified into a mechanism of self-emancipation and empowerment but that, in reality, participatory surveillance comes in many forms and serves many purposes, some of which are more sinister than others. She subsequently concludes that 'in the

[468] Ibid 215.
[469] Romele et al (n 462) 216-217.
[470] Ibid 208.
[471] Siva Viadhyanathan (n 429). See also Siva Viadhyanathan, *The Googlization of everything (and why we should worry)* (University of California Press, 2011) 112.
[472] Julie Cohen, 'The surveillance-innovation complex: the irony of the participatory turn' in Barney et al (n 8) at 207.
[473] Ibid 271.

contemporary era of commercial surveillance, careful attention to the context and character of participation is essential.'[474]

Three main approaches to the individual's role in surveillance can be derived from the above overview of the 'participatory surveillance' branch of the third wave: (i) the positive approach that emphasises the entertaining and empowering aspects of surveillance now enjoyed by the individual; (ii) the dystopian interpretation of participation as submission to state and corporate surveillance structures; and, (iii) the middle ground that acknowledges participation but warns against it being over-emphasised and used to facilitate an unjustified extension of the state and corporate gazes. This thesis does not endorse the second approach that construes individuals' participation in digital data exchanges as a form of resignation to more hierarchical structures of surveillance rather than as participation in their own surveillance practices. This approach fails to appreciate the democratisation of surveillance power that has emerged in the digital age and the benefits for civil society accompanying this development, such as the ability of individuals to return the gaze of the watcher to question and challenge established powers relationships. On this basis, this thesis endorses the positive approach to participatory surveillance in so far as it underlines the enjoyment and ownership of surveillance by the individual. However, in agreement with the third approach, the participatory turn must not be over-emphasised so that it becomes facilitative of unjustified state (and corporate) surveillance regimes. Participatory surveillance must be positioned in such a way that its benefits can be enjoyed without simultaneously being manipulated to extend the institutional gaze. The extent to which this has been achieved by the IP Act is examined in the following chapter.

3.4 Summary

From the above overview of third wave surveillance theories, the following characteristics of contemporary surveillance brought about by technocultural change are identified: the state, the corporation, and the individual are now actors of

[474] Ibid 281.

surveillance; surveillance is disciplinary, controlling, entertaining and empowering; it is hierarchical and non-hierarchical; it is visible and physical, as well as numerical and hidden.[475] First and second wave surveillance characteristics are thus still visible in the contemporary surveillance landscape but are now accompanied by a non-vertical axis of surveillance that has emerged from individuals' engagement with ICTs like social media and smartphones. Non-vertical surveillance can be entertaining and beneficial for the individual, while also being intersected by more vertical practices of surveillance for purposes of discipline and control. Thus, it is important not to over-emphasise the participatory turn in surveillance as an 'enlightened form of self-emancipation' as it risks neutering the negative connotations associated with surveillance which, in turn, risks positioning it as an 'activity exempted from legal and social control.'[476] Fuchs similarly warns of notions of participatory surveillance being used to 'downplay the actual repressive power of capitalism and the state.'[477] Therefore, the participation of the individual needs to be properly positioned under laws regulating surveillance so that the benefits of the contemporary surveillance can be enjoyed without being used to unjustifiably extend the gaze of the state or corporation. The IP Act's approach to participation is established in Chapter 4 and critically assessed in terms of its impact on privacy in Chapter 5.

Part 2 Sites of third wave surveillance

This part illustrates the characteristics of the contemporary surveillance landscape identified in Part 1 via an examination of social media and smartphones as 'sites of third wave surveillance.' These have been selected on the basis that they showcase the various different relationships and cultures of surveillance coursing through the contemporary landscape and the legal implications that flow from it. Three legal implications are demonstrated: (i) the participation of the individual; (ii) the collapse of traditional dichotomies; and, (iii) the need for a group privacy right.

---

[475] As also noted by Galic et al, 'Surveillance theory and its implications for law' (n 64) 740.
[476] Cohen, 'The surveillance-innovation complex' (n 472) 270.
[477] Christian Fuchs, 'Surveillance and critical theory' (2015) 3 Media and Communication 6, 7.

First, smartphones and social media illustrate the extent to which digital data exchanges have become integral to everyday life and how they have enabled the individual to play an active role in the surveillance landscape. By conceptualising the individual's use of social media and smartphones as surveillance, the democratisation of surveillance power (and its benefits) in the digital age is demonstrated. By underlining the individual's ownership of surveillance (for entertaining and empowering purposes as opposed to a solicitation or resignation to the state or corporate gaze), this thesis argues that expectations of privacy against institutional watching can persist even within realms of exposure (like social networking sites). Consequently, the law's failure to properly position the participation of the individual risks: (i) failing to recognise expectations of privacy where necessary, and (ii) undermining the benefits bestowed on civil society by a more democratised surveillance landscape.

Second, smartphones and social media showcase the collapse of traditional boundaries, especially that of the public-private dichotomy. The public-private dichotomy functions as a 'boundary-marking concept' which are 'concepts that can function to mark limits of acceptability, reflecting fundamental assumptions about human existence.'[478] For example, in Chapter 2 it was demonstrated that whilst privacy can exist outwith traditionally private spaces like the home, it is significantly more restricted.[479] Whilst this division between public and private space (and information) was more adequate in previous analogue eras, this distinction has become difficult to maintain in the digital age where traditionally in-house activities are being transferred outwith the home and into (virtual) public space. Accordingly, laws based on this increasingly outdated boundary-marking concept pose serious risks to privacy by failing to provide adequate protection to private life outwith the classic bastion of the home.

[478] Bert-Jaap Koops, 'On legal boundaries, technologies, and collapsing dimensions of privacy' (2014) 3 Politica e Societa 247, 248.
[479] See discussion of *Peck v UK* and *Friedl v Austria* in Chapter 2, section 1.2.1 and 1.2.2.

Third, these 'sites of third wave surveillance' underline the growing need for a group privacy right. The proliferation of social media and smartphones has led to an explosion of individuals' data exhaust. Whilst not all of the information generated is necessarily 'private,' its aggregation into vast databases and subsequent analysis via Big Data techniques can be highly revealing. Indeed, the value of metadata was underlined by Snowden who showed the extent to which state surveillance regimes are now geared towards the collection of information about 'an undefined number of people during an undefined period of time without a pre-established reason.'[480] Thus, it is no longer just the individual or suspect group targeted by surveillance, but also vast groups of persons. However, as demonstrated in Chapter 2, there exists limited access to privacy at a group or collective level under Article 8 which is largely oriented around the individual and their specific interests.[481] This has led to calls for the law

> 'to be adjusted, and possibly extended in order to pay attention to the actual technological landscape unfolding before us…where risks relating to the use of big data may play out on the collective level, and where personal data is at one end of a long spectrum of targets that may need consideration and protection.'[482]

In support of this stance, the following demonstrates the growing need for a group privacy right in the third wave landscape - where surveillance is both specific and general, targeted and un-targeted.

Having illustrated the reality of the third wave and the legal implications that flow from it, the IP Act's approach to each can subsequently be determined in Chapter 4 before being critically assessed in terms of its protection of privacy under Article 8 ECHR in Chapter 5. This enables a conclusion to be reached as to the suitability of UK surveillance law in the digital age.

---

[480] Van der Sloot (n 351) 216.
[481] See Chapter 2, section 4.
[482] Linnett Taylor, Luciano Floridi, Bart van der Sloot, 'Introduction: a new perspective on privacy' in Taylor et al (n 61) 1.

1 Social media

Social networking sites are defined by Boyd and Ellison as

> '[w]eb-based services that allow individuals to: (1) construct a public or semi-public profile; (2) articulate a list of other users with whom they share a connection; and, (3) view and traverse their list of connections and those made by others within the system.'[483]

The increased visibility of individuals on these sites has led to social media being viewed as 'synonymous with surveillance' within surveillance studies scholarship.[484] There are various different types of surveillance operating on social media that were touched on above, including: peer-to-peer surveillance; self-surveillance; corporate surveillance; and, state surveillance.

Using Facebook as the main example, this section examines the different types of surveillance that exist on this platform to demonstrate the hybridity of actors and purposes of surveillance that is characteristic of the third wave landscape, in particular the individual's participation in surveillance. The following conceptualisation of Facebook as a 'dwelling' also illustrates the collapse of the public-private dichotomy, discussed above, with individuals now carrying out traditionally private (often home-based) activities on these (quasi-) public virtual social networking spaces. Facebook has been selected on the basis that it is the largest social media platform and is 'a public face to a constellation of surveillant agents.'[485] Finally, the need to develop a group privacy right is demonstrated via an analysis of the state's mass social media surveillance that causes harm on more of a collective than personal level.

1.1 Facebook: a dwelling

Facebook was created in February 2004 by Harvard student, Mark Zuckerberg. Although originally created for connecting with peers in Ivy-league colleges in the US,

---

[483] Danah Boyd and Nicole Ellison, 'Social network sites: definition, history, and scholarship' (2007) 13 Computer-Mediated Communication 210, 211.
[484] Daniel Trottier, 'A research agenda for social media surveillance' (2011) 8 Fast capitalism 1.
[485] Ibid 4.

in 14 years it has amassed over two billion users worldwide.[486] Users create and maintain profiles, make connections with other 'users' who then become 'friends,' and share information via statuses which can take the form of text, photographs, website links, or videos. There is also a 'News Feed' feature which displays the activities and interactions of the user's network.[487] The exponential growth in its user base and ubiquity of handheld ICTs, has enabled Facebook to transcend the physical, fixed locations of the desktop computer and be carried around in the hands and pockets of its users; facilitating a perpetual engagement with the site.

Trottier describes Facebook, and social media generally, as a 'lived condition;'[488] a 'dwelling' that 'we live through…and we live on.'[489] The significance of recognising Facebook as a dwelling lies in the substantial transferral of social life online from typically more intimate (private) settings (like the home), rendering individuals considerably more visible to their peers – and whoever, or whatever, else is dwelling there. With this new visibility has come new surveillance opportunities for the state, the corporation, and the individual. Whilst some of these practices are participated in and even desired by the individual, others are more sinister, discreet and unanticipated. This is recently demonstrated by the data harvesting of 82 million Facebook profiles by political consulting firm, Cambridge Analytica, without users' consent or knowledge.[490]

The following explores the vertical and non-vertical axes of surveillance carried out on Facebook and the interaction between the two. This demonstrates the hybridity of the third wave landscape where actors and purposes of surveillance converge.

---

[486] Facebook Statistics (*Facebook*, 31 March 2018) <https://newsroom.fb.com/company-info/> accessed 6 June 2017.
[487] This was introduced in 2006 and received a significant level of backlash with users contesting its apparent invasion of privacy.
[488] Daniel Trottier, 'Interpersonal surveillance on social media' (2012) 37 Canadian Journal of Communication 319, 321.
[489] Trottier (n 8) 2.
[490] Issie Lapowsky, 'Facebook exposed 87 million users to Cambridge Analytica' (*Wired*, 4 April 2018) <https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/> accessed 2 May 2018.

1.2 Participatory surveillance

This section conceptualises the individuals' digital data exchanges on Facebook in terms of participatory surveillance.[491] Two forms of participatory surveillance are considered: (i) peer-to-peer surveillance, and (ii) autobiographical surveillance. An examination of each demonstrates the different purposes for which individuals now use surveillance and the benefits that this democratisation of surveillance has bestowed on civil society. Therefore, this section underlines the importance of properly recognising the actorship of the individual so that participation is not misinterpreted to extend the unjustified gaze of the institutional watcher.

1.2.1 Peer-to-peer surveillance

The extent to which peers now 'watch over' one another on social media has prompted surveillance studies academics 'to unpack the ongoing eavesdropping, investigation, gossip, and inquiry that constitutes information gathering by people about their peers.'[492] As set out above, Andrejevic's concept of lateral surveillance or 'peer-to-peer monitoring' refers to the use of surveillance by individuals (as opposed to public or commercial actors) to keep track of one another.[493] He lists three main categories of persons' subject to such horizontal watching: romantic interests, family and friends, and acquaintances.[494] Whilst Andrejevic does not apply his theory to social media (likely due to the time of writing), later quantitative studies have shown that this type of surveillance is prevalent on Facebook. For example, Lampe et al conducted a study on a college campus and determined that Facebook was predominantly used for 'social searching' – finding out information on individuals they already had a previous, offline, connection with - as opposed to 'social browsing' where Facebook is used to seek out new connections.[495] They specifically note the surveillance function of 'social searching' on Facebook as it 'allows an individual to track the actions, beliefs and interests of the larger groups to which they belong.'[496] Joinson's study similarly

---

[491] For 'participatory surveillance' see Part 1, section 3.3.
[492] Marwick (n 451).
[493] Andrejevic (n 439) 481. See Part 1, section 3.3.
[494] Ibid 488.
[495] Lampe et al (n 450) 169.
[496] Ibid 167.

found that, after keeping in touch with friends, the 'social searching' function of Facebook was the second most commonly reported motivation behind individuals' subscription to the platform, demonstrating the extent to which it is used to watch over one's peers.[497]

Individuals also refer to peer monitoring on Facebook in surveillance-related terms. For example, 'stalking' and 'creeping' are commonly used to describe the monitoring of other users on the platform. Trottier's analysis of the usage of these terms found that 'creeping' was viewed as a milder form of 'stalking' that constituted 'a more involved and targeted way of using Facebook.'[498] Examples of creeping could, therefore, include browsing another user's profile, photos and statuses.[499] 'Stalking,' on the other hand, is distinguished as being a 'little bit more aggressive,' for example, if a user were to purposefully and consistently monitor a particular profile as opposed to merely falling upon a profile out of serendipity.[500]

Trottier, who describes peer monitoring on Facebook as 'interpersonal surveillance,' argues that although some exercises of surveillance (like 'stalking') are perhaps more unwanted than others, users generally come to expect and accept that this practice exists because they do it themselves.[501] Trottier thus argues that the gaze is 'normalised because users act as both watcher and watched.'[502] Marwick similarly argues that the reciprocity of peer-to-peer surveillance on Facebook 'engenders both disclosure and concealment' as the individual monitors other users' content in order to contextualise their own sharing, in other words, they internalise the gaze of other watchers in order to regulate their own behaviour. However, this normalisation of the gaze and expectation of surveillance by other Facebook users does not necessarily extend to increase users' expectations of surveillance by states and corporations that also dwell in this space. The gaze of states and corporations differs significantly from the average

---

[497] Adam Joinson, 'Looking at, 'looking up' or 'keeping up with' people? Motives and use of Facebook (2008) CHI-2008 Proceedings 1027.
[498] Trottier, 'Interpersonal surveillance on social media' (n 505) 324-325.
[499] Ibid 325.
[500] Ibid.
[501] Ibid.
[502] Trottier, 'Social media as surveillance' (n 8) 61.

Facebook user (ie discipline and control instead of entertainment and sociality) and is is carried out more discretely and covertly. Thus, it is important that the participation of the individual in peer-to-peer surveillance on social media and the subsequent expectation of being watched by other users is recognised for what it is - a way of enhancing sociality and developing relationships - and not misconstrued as blanket acceptance of surveillance by more hierarchical watchers who also occupy this dwelling.

1.2.2 Autobiographical surveillance

This section conceptualises the individual's sharing of information about him/her-self on social media as a form of self-surveillance called, 'autobiographical surveillance.' This concept is used to illustrate the benefits of surveillance to the individual that are facilitated by social media. In addition, the following description of the types of information individuals share on social media demonstrates the extent to which the boundary between public and private (information) has become permeable in the digital age with 'the privatisation of the public, and publicisation of the private.'[503]

Harcourt writes that 'our digital self is a narrative self, one that we construct through our presentation of self and telling of stories.'[504] The 'narrative self' is particularly evident on social media. For instance, on Facebook users: post statuses about their emotions, activities, thoughts, and beliefs; share pictures documenting their life (and that of others); and, 'check-in' to share their geographical location. Facebook users can also share a 'life event' to broadcast milestones in their life to their followers. They can either create their own 'life event' or select an event from a list of categories (eg 'work and education,' 'family relationships,' 'home and living,' and so on). Within this list of categories, there are over forty life events to choose from. The prefix 'autobiographical' thus serves to capture users' transcription of real-life events into a prescribed, chronological, digital format that is amenable to sharing with a wide audience.[505] Drawing from Marwick's theory of 'social surveillance,' the following

[503] Koops (n 478) 257.
[504] Harcourt (n 12) 128.
[505] This has also been referred to as 'lifestreaming,' see Marwick (n 451) at 389.

conceptualises users' autobiographical performances on social media as a type of self-surveillance that serves a variety of self-serving purposes, including: entertainment, the development of interpersonal relationships, and a stronger sense of self.

Marwick defines 'social surveillance' as 'the ongoing eavesdropping, investigation, gossip and inquiry that constitutes information gathering by people about their peers, made salient by the social digitisation normalised by social media.'[506] Acknowledging that some may question whether such activities are rightly considered 'surveillance,' she underlines that 'social surveillance leads to *self*-management and direction on the part of social media users,' which is a well-accepted characteristic of surveillance.[507] On this basis, Facebook (and social media generally) may be seen as having panoptic-type effects on its users who 'monitor their digital actions with an audience in mind, often tailoring social media content to particular individuals.'[508] However, the gaze of one's peers is internalised, as opposed to that of the unobservable central watcher of the Panopticon. The self-narration and self-scrutiny of the self on social media is thus conceptualised here as a type of participatory surveillance referred to in this thesis as 'autobiographical surveillance.'

With regard to the purpose of autobiographical surveillance, this thesis argues that it helps to develop a stronger sense of self and identity. This is supported by John Thompson's theory that the narration of one's life to others is fundamental to identity formation:

> 'To recount to ourselves or others who we are is to retell the narratives – which are continuously modified in the process of retelling – of how we got to where we are and of where we are going from here. We are all the unofficial biographers of ourselves, for it is only by

[506] Ibid 382.
[507] Ibid 381. As shown in the discussion of first wave surveillance theories in Part 1, section 1 of this Chapter.
[508] Marwick (n 451).

> constructing a story, however loosely strung together, that we are able to form a sense of who we are and of what our future may be.'[509]

This is also echoed in Foucault's 'Technologies of the self,' where he argues that

> 'one of the main features of taking care involved taking notes on oneself to be reread, writing treatises and letters to friends to help them, and keeping notebooks in order to reactivate for oneself the truths one needed…Taking care of oneself became linked to constant writing activity. The self is something to write about, a theme or object (subject) of writing activity.'[510]

Therefore, if we view social media as the modern digital (and more public) version of the diary or notebook, the function of autobiographical surveillance becomes the development and care of one's self. This is also supported by Foucault's work on the confessional society where he argues that the confession has 'spread its effects far and wide' from its religious origins to more secular forms such as policing, medicine, and family life as a means of caring for the soul.[511] Foucault views the confession as integral to pastoral power which 'cannot be exercised without knowing the inside of people's minds, without exploring their souls, without making them reveal their innermost secrets.'[512] Thus, for Foucault, the act of confessing is closely tied to surveillance as it reveals all that is hidden to a powerful other and enables them to be ruled, guided, punished, counselled, and directed.'[513] Harcourt similarly notes the resemblance between sharing on Facebook to 'earlier forms of avowal, of examination of the self, of penitence even.'[514] However, in the past confessions were made to a

---

[509] John Thompson, *The media and modernity: a social theory of the media* (Stanford University Press, 1995) 210.
[510] Michel Foucault, Luther Martin, Huck Guttman, Patrick Hutton, *Technologies of the self* (University of Massachusetts Press, 1988) 27..
[511] Michel Foucault, *The history of sexuality volume I: an introduction* (Vintage Books, 1978).
[512] Ibid 59.
[513] Ibid.
[514] Harcourt (n 12) 100.

higher power or at the very least to one anointed individual (ie a priest), as opposed to vast audiences online.

Conceptualising Facebook as a confessional lends support to Koskela's aforementioned 'empowering exhibitionist' movement with individuals embracing exposure as a means of emancipation from inner turmoil and using visibility to illicit assurance, acceptance, and absolution from their peers.[515] In this way, digital data exchanges on social media can be viewed as the active participation in one's own surveillance for the purposes of self-care and self-actualisation.

However, curtailing this empowering account of autobiographical surveillance is that a user's story can have many different authors with a user's autobiography often informing that of another user. For example:

> User A uploads a picture of themselves at a party which also features User B. User A can further augment User B's visibility by tagging her in that picture meaning that the image will be shared to User B's audience as well as to User A's. User A may also tag User B in posts that she thinks User B might like or find funny. This tag is then shared to both users' audiences via the 'News Feed.' In doing so, the audiences of both users are able to piece together a mosaic of User B's character. For example, if User B is frequently tagged in photos at parties, inferences might, rightly or wrongly, be made as to B's lifestyle or character.

In this sense, a user's autobiography can become 'biographical' with the individual possessing limited control over what information is put 'out there' by these other authors. Trottier and Lyon refer to this process as 'collaborative identity construction' which allows 'users to share information about their friends with those friends.'[516]

---

[515] Koskela (n 456). See Part 1, section 3.3.
[516] David Lyon and Daniel Trottier, 'Key features of social media surveillance' in Christian Fuchs (ed) *Internet and surveillance: challenges of Web 2.0* (Routledge, 2012) 94.

Evidence shows that a desire to control what is already 'out there' is a major motivation behind individuals' subscription to Facebook.[517] Trottier subsequently contends that the 'intentional visibility' heralded by scholars like Albrechtslund and Koskela as self-empowering, 'cannot be disassociated from unanticipated exposure.'[518] Therefore, visibility on social media is something of a paradoxical condition 'managed by the individual that assists him in gaining recognition but that also contributes to his exposure and supervision.'[519] Harcourt similarly notes: 'we embrace digital exposure with a wild cacophony of emotions, ranging from fetishism and exhibitionism for some to discomfort, hesitation, and phobia for others.'[520] Enhanced visibility on social media thus warrants a vigilant 'care of the virtual self'[521] as users are responsible for their own exposure as well as that of others.[522]

By conceptualising the individual's exposure on social media as an exercise of self-surveillance, the notion of 'autobiographical surveillance' demonstrates: (i) the individual's ownership of surveillance within the third wave landscape, and (ii) the benefits of surveillance as an apparatus for self-care and sociality. In doing so, this concept challenges the construction of individuals' exposure on social media as an antipathy toward privacy or resignation to the gaze of states and corporations, and enables expectations of privacy to persist within these realms of exposure. This is also supported by the fact that not all of the information 'out there' is actively contributed by the individual herself. Therefore, it is important that laws regulating surveillance properly position the role of the individual in the contemporary surveillance landscape so that they are attuned to the technocultural realities of the digital age and provide adequate protection to privacy where necessary.

---

[517] Trottier, 'Interpersonal surveillance on social media' (n 488) 322-323.
[518] Ibid 320.
[519] Tali Hatuka and Eran Toch, 'Being visible in public space: the normalisation of asymmetrical visibility' (2017) 54 Urban Studies 984, 988.
[520] Harcourt (n 12) 110.
[521] Jennifer Whitson and Kevin Haggerty, 'Identity theft and care of the virtual self' (2008) 37 Economy and Society 572.
[522] Trottier, 'Interpersonal surveillance on social media' (n 488) 328-330.

1.3 Vertical social media surveillance

Building on the aforementioned theme of 'unanticipated exposure,' this section demonstrates how the design of Facebook facilitates unique surveillance opportunities for corporations and states who now also occupy the Facebook 'dwelling.' This demonstrates the hybridity of the current third wave landscape where first and second wave surveillance continue to operate, and the subsequent need for the law to stem the flow of the unjustified gaze into these realms.

1.3.1 Corporate social media surveillance

Whilst corporate surveillance is not the main focus of this thesis, the following provides a brief overview of corporate social media surveillance to demonstrate the hybridity of the contemporary landscape. It demonstrates how the individual's participation in surveillance via digital data exchanges on these platforms can be used to enhance and inform more hierarchical structures of surveillance, thereby undercutting the democratising potential of social media brought about by the reciprocity in watching illustrated above. In addition, the gaze of the corporation is increasingly capitalised on by the state.[523]

In constructing Facebook as a 'dwelling' Trottier employs De Certeau's distinction between the owners of enclosures and those who dwell there to demonstrate the extent to which corporations benefit from the sharing of personal information on social media.[524] According to De Certeau, the owner has the power to determine and regulate the use of a space whereas the dweller merely resides there.[525] The dweller can employ tactics for life within the enclosure but these can be observed, subsumed, or eliminated by the owner who possesses ultimate control over the use of the space. Consequently, 'a user's tactics become an owner's strategies.'[526]

---

[523] For example, under the IP Act corporations can be placed under a duty to assist in the implementation of warrants. See IP Act 2016, s 43. This is discussed further in Chapter 4.
[524] Trottier, *Social media as surveillance* (n 8) 53.
[525] Michel de Certeau, *The practice of everyday life* (1988, University of California Press).
[526] Trottier, *Social media as surveillance* (n 8) at 57, citing from Lev Manovich, 'Software takes command' (unpublished, 2008) <http://softwarestudies.com/softbook/manovich_softbook_11_20_2008.pdf> accessed 5 July 2017.

By applying De Certeau's distinction between owners and dwellers to Facebook, Trottier shows that despite the democratisation of surveillance on the platform, the owner's birds-eye-view of the dwelling ultimately privileges their position over the users' (the dwellers).[527] Thus, despite the opportunity for users to customise their own experience of Facebook, the tactics used can generate a kind of information that can be recorded by the service provider. For example, a user might modify their privacy settings to hide information from other users but this tactic remains visible and recordable to the owners of Facebook. Therefore, despite the reciprocity in surveillance between users, an asymmetry of surveillance persists and even thrives on social media where 'the transformation of everyday life into a kind of enclosure' enables information to be 'extracted and turned into a brokered raw material.'[528]

In addition, Facebook does not only watch dwellers within its own enclosure, having developed a variety of techniques and programs to carry out internet-wide surveillance of its users. For example, in 2007 Facebook introduced the 'Beacon' programme to 'try to help people share information with their friends about things they do on the web.'[529] In effect, it was an advertising system that reported back to Facebook any user activity on third party sites that were participants of Beacon. The information gathered would then be published on an individual's 'news feed' and shared with other users. This was carried out even when the individual was not using Facebook and without their knowledge. Additionally, there was no option to opt-out of the programme. For these reasons, Beacon received significant backlash due to concerns over privacy and, following the class action lawsuit of *Lane v. Facebook* where the plaintiffs claimed the programme breached various state and federal laws, it was eventually shut down.[530] However, it was shortly replaced by 'Facebook Connect' which prompts users to sign up and log in to third party sites via their Facebook profiles to make 'it easier for you

---

[527] Trottier, *Social media as surveillance* (n 8) 57.
[528] Ibid.
[529] Mark Zuckerberg, 'Thoughts on Beacon' (*Facebook*, 5 December 2007) <https://www.facebook.com/notes/facebook/thoughts-on-beacon/7584397130/> accessed 7 July 2017.
[530] *Lane v Facebook* 709 F.3d 791 (9th Cir. 2013); resulted in Facebook paying a case settlement fund of $9.5m which was used to establish and operate a privacy foundation.

to take your online identity with you all over the Web.'[531] However, it also lets Facebook track and store its users' internet activity, albeit with their permission this time. These programmes thus 'suggest a kind of meta-surveillance, with Facebook watching over other watchers.'[532]

Aside from Facebook, other corporations also carry out their own surveillance on the platform. In terms of marketing, Facebook provides a useful resource for companies to find out information about how their products are rated, to gain new insight into potential gaps in the market, to gain intel on competitors, and to view how their products are being used by consumers. Social media users can reasonably be conceived as unpaid labour with their personal information providing the raw material for developing business strategies. This is captured by concepts of the social media 'prosumer' (content producing consumer)[533] and 'digital labour'[534] which maintain that time spent on social media is 'not simple consumption or leisure time, but productive time that generates economic value.'[535]

Workplace surveillance is also carried out via Facebook with businesses searching and monitoring current and prospective employees via their profiles and interactions with friends on the platform.[536] Whilst the user might be held responsible for restricting access to his or her profile through the modification of privacy settings, as discussed above, unanticipated leaks can still occur due to the aforementioned 'collaborative identity construction' that takes place on social media.

---

[531] Kathy Chan, ' Facebook across the Web' (*Facebook*, 4 December 2008) <https://www.facebook.com/notes/facebook/facebook-across-the-web/41735647130/> accessed 7 July 2017.
[532] Trottier, *Social media as surveillance* (n 6) 7.
[533] Christian Fuchs, 'Social media and capitalism' in Tobias Olsson (ed.) *Producing the Internet: critical perspectives of social media* (Nordicom, 2013) at 34.
[534] See, Trebor Scholz (ed.), *Digital Labour: the internet as playground and factory* (Routledge, 2013).
[535] Christian Fuchs, 'Digital presumption labour on social media in the context of the capitalist regime' (2014) 23 Time and Society 97, 98.
[536] Surveillance of employees on social media was recently recognised by the Article 29 Working Party which published guidance saying that 'in-employment screening of employees' social media profiles should not take place on a generalised basis,' Article 28 Data Protection Working Party, 'Opinion 2/2017 on data processing at work' (8 June 2017) 17/EN WP 249.

Corporations can also maintain a presence on Facebook as a dweller to enhance their customer relations, monitor their reputation, and respond to complaints from customers. With regard to the latter, social media offers a particularly useful platform for the consumer as companies have become acutely aware of the precariousness of their reputation that comes with their enhanced visibility on social media. Delta airlines, for example, has been subject to extensive criticism following various social media attacks on their treatment of passengers. One such scenario involved the removal of YouTube blogger, Ahmed Saleh, from a Delta airways plane for speaking Arabic on the phone to his mother and making other passengers feel 'uncomfortable.' Saleh proceeded to film his removal from the plane and post the video on social media. Within minutes it was shared with thousands and Delta received significant criticism as a result.[537]

Corporate social media surveillance *can* be beneficial for the individual. For example, by monitoring pages 'liked' by the user, products and brands they might like can be suggested to them. However, this is countered by Pariser's concept of the 'filter bubble' which warns that

> 'personalisation filters serve up a kind of invisible autopropaganda, indoctrinating us with our own ideas, amplifying our desire for things that are familiar and leaving us oblivious to the dangers lurking in the dark territory of the unknown.'[538]

Thus, whilst the filtering of relevant information to Facebook users might be useful to the individual, it can also carry harmful consequences for civil, democratic society such as the loss of serendipity. This, in turn, can result in the crystallisation of one's

---

[537] BBC News, 'Ahmed Saleh kicked off Delta air lines flight' (*BBC News online*, 23 December 2016) <http://www.bbc.co.uk/news/uk-38395185> accessed 16 August 2017. See also, BBC News, 'Delta hits back against Conservative author Ann Coulter' (*BBC News online*, 17 July 2017) <http://www.bbc.co.uk/news/world-us-canada-40635993> accessed 16 August 2017.
[538] Eli Pariser, *The filter bubble: what the internet is hiding from you* (Penguin, 2012) 15.

preconceptions as individuals fail to encounter random experiences that challenge and develop their ideas and opinions.[539]

In addition, corporate surveillance on Facebook can also harm those who fail to conform to certain expectations. This is captured by Oscar Gandy's work on 'rational discrimination' which illustrates how

> 'segments of the population that are already vulnerable become further victimised through the strategic use of discriminatory algorithms in support of identification, classification, segmentation, and targeting.'[540]

For example, it was revealed that Facebook let advertisers exclude users by race which was used especially in relation to employment, housing, and credit advertisements.[541] Therefore, there is also a crystallisation of discrimination and exclusion.

In light of the above, it can be argued that the democratising potential of social media brought about by the reciprocity in watching, is undercut by the opaque surveillance techniques of the service provider and other corporations operating on these platforms. Therefore, although presented as a site of interactivity to users, Trottier argues that social media users are merely a 'growing mass of unpaid labour' who not only submit their own personal information but also watch over other people's content.[542] This is supported by Poster's concerns over the increased focus on personal life which used to be a remainder of institutional action and scrutiny.[543] Now, however, it appears that

---

[539] See also Sunstein's work on how the Internet can be used to create 'echo-chambers' – to listen and speak only to the like-minded' - in Cass Sunstein, *Republic.com 2.0* (Princeton University Press, 2009).
[540] Oscar Gandy, 'Consumer protection in cyberspace' (2011) 2 Triple C 175, 175.
[541] See Julia Angwin, Terry Pravis Jr, 'Facebook lets advertisers exclude users by race' (*ProPublica*, 28 October 2016) <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race> accessed 16 August 2017.
[542] Trottier (n 14) 57.
[543] Mark Poster, 'Consumption and digital commodities in the everyday' (2004) 18 Cultural Studies 409.

the transferral of social interactions online has facilitated the 'monetisation of personal information' and the erosion of space previously owned by the individual.[544]

In this sense, social media can be viewed as a mechanism through which corporations are better able to enclose and influence and control the individual's decision-making. The legal significance of this lies in the greater role to be played by the law in protecting this 'growing mass of unpaid labour' from exploitation. In order to do so, however, the law would have to relinquish its grasp on the private-public dichotomy and recognise that

> 'no longer can we take for granted that intrusions *inside* the classic bastion of the private sphere are graver than intrusions into the private sphere that remain *outside* of these bastions.'[545]

Alternatively, it could be argued that the individual, in actively placing their personal life online, has voluntarily submitted themselves to the will of the owner or, in the words of La Boetie, has placed themselves under 'voluntary servitude.'[546] In which case, 'in order to have liberty nothing more is needed than to long for it…only a simple act of the will is necessary.'[547] According to this argument, users would need only to unsubscribe from social media to resist such controlling practices of surveillance. However, this thesis rejects this approach on the basis that refraining from social media is not a viable or desirable solution to 'unanticipated exposure' as it fails to acknowledge and respect the prevailing surveillance culture - where watching has become 'part of a way of seeing and of being in the world…of a whole way of life.'[548] The individual's participation in surveillance culture needs to be respected as an expression of ownership of surveillance rather than being misconstrued as resignation to or acceptance of the rhizomatic gaze of the corporation.

---

[544] Trottier, *Social media as surveillance* (n 8) 57.
[545] Koops (n 478) 257.
[546] See Part 1, section 3.3.
[547] La Boetie (n 467) 44.
[548] Lyon, *The culture of surveillance* (n 1).

1.3.2 State social media surveillance

This section examines the use of social media intelligence ('SOCMINT') by law enforcement agencies and intelligence organisations to demonstrate the extent to which state surveillance now relies on the individual's participation in digital data exchanges. It argues that a failure to properly position the individuals' participation in surveillance culture risks: (i) failing to recognise expectations of privacy where necessary, and (ii) undermining the benefits bestowed on civil society by a more democratised surveillance culture. These risks are also posed by a rigid administration of the public-private dichotomy which enables the state's gaze to seep more easily into the individual's private life *online* than it is into the 'classic bastion of the private sphere.'[549] This is despite potentially more revealing information now being available on one's social media profile than in one's home. This is not to say that greater legal protection of the home or traditional private space is unwarranted, but rather that the hierarchy of harm based on this dichotomy poses serious risks to personal privacy in the digital age. Finally, the mass surveillance of SOCMINT illustrates the threat posed to privacy on a collective level and the subsequent need for a group privacy right to be developed.

1.3.2.1 SOCMINT

The term 'SOCMINT' refers to the use of social media by public bodies as a source of intelligence.[550] The term was used in a report published in response to the London riots in August 2011 on the failure of police and intelligence agencies to harness valuable intelligence flowing through these 'vast digital social commons.'[551] SOCMINT can be a form of 'open source intelligence' ('OSINT') which 'refers to a process whereby police or other investigative agencies gather and analyse data that are in principle accessible to any organisation or individual.'[552] Thus, open SOCMINT is social media

---

[549] Koops (n 478) 257.
[550] 'SOCMINT' used in Sir David Omand, Jamie Bartlett, Carl Miller, '#intelligence' (*Demos*, 2012) <https://www.demos.co.uk/files/_Intelligence_-_web.pdf?1335197327> accessed 10 July 2017.
[551] Omand et al, ibid, 9;
[552] Daniel Trottier, 'Open source intelligence social media and law enforcement: visions, constraints and critiques' (2015) 18 European Journal of Cultural Studies 530, 531. For an extensive list of examples of OSINT see Robert Steele's definition in 'United States Marine Corps Comments on Joint Open Source Task Force Report and Recommendations' (1992)

content that is not protected by privacy settings (be it intentionally or ignorantly). It follows that some 'closed' SOCMINT is information gleaned from private profiles and 'direct mails' (private communications on social media).

1.3.2.2 Open SOCMINT

There are various different ways in which open SOCMINT is used by intelligence agencies and law enforcement. For example, an investigating agent can simply log on to a social media site, search for a specific target, and view or monitor their public profile or interactions with friends insofar as privacy settings allow. Alternatively, if a target's profile is private, due to the aforementioned 'collaborative identity construction,' an agent could gain intelligence indirectly by monitoring the profiles of a target's 'friends' (if public). Police departments now also increasingly maintain a presence on social media via their own profile pages where they can both receive and disseminate information. Therefore, like the corporation, the state can now also occupy social media as a 'dweller' to enhance its surveillance reach.

In addition to the above techniques, law enforcement departments have been set up to carry out mass surveillance of open SOCMINT. For example, Scotland Yard ran an 'all source hub' during the 2012 London Olympics to monitor social media. A 'National Domestic Extremism Unit' ('NDEU') has also been established within the Metropolitan police to scan SOCMINT 24 hours a day, 7 days a week, 'to provide intelligence on domestic extremism and strategic public order issues in the UK.'[553] Such departments use various different techniques and software to harness vast amounts of information from these platforms, such as: 'web crawlers' or 'web spiders' to browse the Internet for specific words and phrases that have been selected by an investigating agent, and; 'sentiment-analysis technology', which is used to assess the emotional tenor of text, like a user's status update. The establishment of such departments and techniques demonstrates the extent to which state surveillance is now geared towards watching the un-targeted mass as opposed to just the specified

---

<http://www.oss.net/dynamaster/file_archive/060324/9906ba66ee5fe750bb8fe5712b1e20e7/92%20Jan%2011%20Steele%20on%20IC%20OSINT.pdf> accessed 11 July 2017.

[553] National Police Chief's Council, 'National Domestic Extremism Unit' (*NPCC)* <http://www.npcc.police.uk/NationalPolicing/NDEDIU/AboutNDEDIU.aspx> accessed 12 July 2017.

individual – as well as the extent to which the explosion of personal data traffic in the digital age has facilitated this approach. This is further demonstrated in Chapter 4 via an analysis of the IP Act's approach to the participation of the individual.

However, the above techniques have proven problematic as computers struggle to distinguish sarcastic or jovial comments from real threats. For example, in 2012 two British tourists were interrogated by Homeland Security counter-terrorism officials concerning Facebook posts that stated they were going to be 'diggin up Marilyn Monroe' and 'destroying America.'[554] However, it transpired that the officials were unaware that the Marilyn Monroe comment was a reference to a cartoon comedy ('Family Guy') and that 'destroy' was a British colloquialism for 'party.' Therefore, bringing social media content into the fold of OSINT (and the technologies that go with it) risks losing the context in which posts and comments are originally shared and wrongfully recasting them as criminal acts and evidence.[555] This subsequently demonstrates how the individual's participation in digital data exchanges can be used to inform disciplinary structures of surveillance and how this can destruct the individual's enjoyment of participatory surveillance.

With regard to the legality of open SOCMINT practices under Article 8(1); Chapter 2 established that whilst expectations of privacy can exist in public and over public information, they are significantly reduced.[556] Consequently, more would have to occur than the mere monitoring of a public profile in order for Article 8(1) to be engaged, such as the creation of a permanent record or the processing of the information in such a way that was not foreseeable to user.[557] Therefore, whilst the

---

[554] See Katie Zezima, 'The secret service wants software that detects sarcasm. (Yeah, good luck.)' (*The Washington Post*, 3 June 2014) <https://www.washingtonpost.com/politics/the-secret-service-wants-software-that-detects-sarcasm-yeah-good-luck/2014/06/03/35bb8bd0-eb41-11e3-9f5c-9075d5508f0a_story.html?utm_term=.4f2f5c58bbe6> accessed 2 August 2017.
[555] As noted by Trottier, 'Open source intelligence social media and law enforcement' (n 552) at 535. See also the case of *Paul Chambers v Director of Public Prosecutions* [2012] EWHC 2157 in which the appellant was arrested and convicted (although the conviction was later quashed) for tweets joking that he was going to blow Robin Hood airport 'sky high' following its closure after snowfall on the basis that his statements were of a 'menacing character' and alarmed airport staff enough for them to report it.
[556] See further Chapter 2, sections 1.2.1 and 1.2.2.
[557] Ibid.

retention or processing of open SOCMINT would require a basis in law under Article 8(1), it is unlikely that this would be the case for the mere monitoring of this intelligence. The extent to which the IP Act adheres to human rights in its surveillance of open SOCMINT is examined in Chapter 5. Although, as no explicit reference to SOCMINT (open or closed) is made in the Act, this analysis is carried out via an examination of its data-focussed powers under which open SOCMINT would likely fit. This enables a conclusion to be reached as to the suitability of both the IP Act *and* the ECHR in terms of their positioning of participation and, therefore, their protection of privacy in the digital age.

1.3.2.3 Closed SOCMINT

Compared with open SOCMINT, surveillance of closed SOCMINT constitutes an automatic interference with Article 8(1) as it requires the use of interception or equipment interference[558] (which has been deemed equivalent to interception by the ECtHR).[559] Accordingly, the surveillance of closed SOCMINT must fulfil the legality and necessity requirements listed under Article 8(2). The extent to which the IP Act adheres to these standards is determined in Chapter 5.

In terms of how closed SOCMINT is gathered, Snowden revealed that highly unconventional methods have been used by intelligence agencies. For example, the data-mining program 'PRISM' launched in 2007 allowed the NSA to tap directly into the servers of major service providers such as Yahoo, Google, Facebook, YouTube, Skype, and Apple (see Figure 1, below). The investigating agent simply required a 'reasonable suspicion that one of the parties was outside the country at the time the records were collected by the NSA,' and did not require a legal warrant or authorisation.[560] PRISM was also used in conjunction with 'XKeyscore' which enabled analysts to search through the vast data gathered - ergo its description as the

[558] See analysis of *Malone v UK* in Chapter 2, section 1.1.
[559] See Chapter 5, section 2.2.1 for discussion of interception and EI. See analysis of *Malone v UK* in Chapter 2, section 1.
[560] Glenn Greenwald and Ewen MacAskill, 'NSA Prism program taps in to user data of Apple, Google and others' (*The Guardian*, 7 June 2013) <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed 2 August 2017.

'NSA's Google for the world's private communications.'[561] The programs released by Snowden were undertaken in partnership with allies part of the 'Five Eyes' alliance.[562] The GCHQ program 'Tempora,' for example, was launched in 2007 and gathered data through interceptors placed on around 200 fibre-optic cables running in and out of the UK.[563] This included internet traffic between the US and Europe, hence GCHQ's description of the program as 'mastering the internet.'[564] The data gathered was then shared with the NSA and sifted through by agents from both intelligence agencies on the basis of specific searches relating to trigger words, email addresses, targeted persons, and so on.[565]

Figure 1: Source: *The Washington Post*, 6 June 2013

Providers	**Information collected**
Microsoft	E-mail
Google	Chat – video, voice
Yahoo	Videos
Facebook	Photos
PalTalk	Stored data
YouTube	VoIP (voice over internet protocol)
Skype	File transfers
AOL	Video conferencing
Apple	Notifications of target activity – logins etc.
	Online social networking details
	'Special requests'

[561] Morgan Marquis-Boire, Glenn Greenwald, Micah Lee, 'XKeyscore' (*The Intercept*, 1 July 2015) <https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/> accessed 12 July 2017.

[562] The 'Five Eyes' alliance was established in 1946 between the intelligence agencies of the US, UK, Australia, Canada, and New Zealand. Under the agreement, interception, collection, gathering, analysis and decryption is carried out by each state and information is shared between the allies by default.

[563] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies, James Ball, 'GCHQ taps fibre-optic cables for secret access to world's communications' (*The Guardian*, 21 June 2013) <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> accessed 2 August 2017.

[564] Ibid.

[565] Prior to PRISM, a similar program called 'Total Information Awareness' ('TIA') was established following 9/11 and aimed at collecting as much information on as many people as possible, to then be stored on a large-scale database which could be scoured by state officials to identify terrorist threats. However, it was met with considerable backlash within the popular media and the program was eventually defunded in 2003. Clearly, however, TIA continued to operate in the form of PRISM although, interestingly, with fewer safeguards. For information on the history of TIA see Newton Lee, 'The rise and fall of Total Information Awareness' in Newton Lee (ed) *Counterterrorism and cybersecurity* (2nd edn, Springer, 2015) 135-149

The above demonstrates the extent to which individuals' participation in digital data exchanges (to which surveillance is inherent) has worked to provide a supporting infrastructure to the vertical axis of surveillance. State surveillance has evidently thrived in the digital age with sites like Facebook making the private life of the individual significantly more accessible. Chapters 4 and 5 underline the risks posed to privacy by the the above mass surveillance powers which continue to operate in the UK under the IP Act, albeit more transparently than pre-Snowden. It is argued in the following chapters that the maintenance of these mass surveillance powers demonstrates a failure to properly position the individual's participation in surveillance culture and, therefore, to attune to the technocultural realities of the digital age which poses serious risks to privacy.

1.4 Summary

The above examination of social media has served to illustrate many of the key characteristics of the third wave identified in Part 1 (section 3), including: the convergence of actorship (the individual, the state, and the corporation); the different purposes of surveillance (discipline, control, and entertainment); and, the existence of both hierarchical and non-hierarchical surveillance in the contemporary landscape. It has also demonstrated how these different practices and axes of surveillance interact with and intersect one another, with the individual's own surveillance practices providing a unique opportunity for corporate and state surveillance on social media. This is supported by Trottier who notes that, 'interpersonal transparency and disclosure is a specific kind of visibility that enhances formal types of surveillance.'[566] In this sense, social media might be conceptualised as something of a surveillant assemblage where once intangible social interactions are converted into digital transactions amenable to subsequent gathering, processing and retention by other individuals, corporations or state agencies. This 'criss-crossing of the gaze' on social media is particularly well illustrated by the '#blacklivesmatter' campaign challenging institutional racism.

[566] Trottier, 'A research agenda' (n 484) 6.

The campaign was established following the acquittal of policeman George Zimmerman, who shot and killed unarmed African-American teenager Trayvon Martin. It was organised on social media and led to nationwide protests across the US. Via the hashtag, victims and witnesses from around the world started sharing their own experiences of racism. These posts frequently showed videos captured by victims on their smartphones depicting first-hand the type of racism suffered at the hands of the police. Thus, social media can be seen as enabling the co-ordination of opposition. However, the American Civil Liberties Union ('ACLU') has recently published findings on social media providers (Facebook, Instagram, and Twitter) that provided users' data to 'Geofeedia' – a social media monitoring company that advertised its services to companies and law enforcement agencies for the tracking of activists of colour.[567]

As well as demonstrating the criss-crossing of the gaze on social media, the above example also shows that, despite the democratisation of the gaze, the owners of the enclosure retain ultimate control over access to and use of the dwelling - possessing a birds-eye-view that enables the tactics of the dweller to be subsumed, harnessed, and exploited by the owner and his friends (who might be other corporations or the state). The question subsequently arises as to what role the law currently plays, and what role it *should* play, in protecting the privacy of the individual (and indeed that of the collective given the mass surveillance of both open and closed SOCMINT), from the disciplinary and controlling gazes operating within these realms of exposure online. This will be considered in Chapter 4 via an examination of the IP Act's approach to the participation of the individual. The impact of this approach on the protection of privacy is then assessed in Chapter 5 via an analysis of the Act under Article 8 ECHR.

[567] Matt Cagle, 'Facebook, Instagram, and Twitter provided data access for a surveillance product marketed to target activists of colour' (*ACLU,* 11 October 2016) <https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target> accessed 13 July 2017.

2 Smartphones

A smartphone is 'a mobile phone that can perform many of the functions of a computer.'[568] Smartphones have many features, such as built in microphones, cameras, GPS, Internet, and can run downloaded applications ('apps'). Apps are typically internet-based and enable individuals to scrutinise different aspects of their life and bodies in 'granular detail – how we sleep, where we go, what we breathe, what we eat, how we spend our time.'[569] The idea of their being an 'app for everything,' is noted by Groening who argues that Apple's commercials 'endeavour to show that any conceivable activity has a corresponding 'app' that can transform the cellular phone into an essential tool for that activity.'[570] The smartphone also facilitates the sharing of information generated by these activities and, as such, has enabled individuals to enhance their visibility in different spaces. However, this data is also broadly accessible to third parties, such as corporate and state bodies. Consequently, there exists a 'bi-directional paradigm – of vertical surveillance and horizontal sharing – [which] contributes to a sense of 'being exposed' in public space.'[571]

This section unpicks the vertical and non-vertical axes of surveillance flowing through smartphones, demonstrating the hybridity of the contemporary surveillance landscape. In addition, this sections shows the various different actors now participating in surveillance and underlines the role of this ICT in facilitating the democratisation of surveillance and the benefits subsequently bestowed on civil society. However, it also demonstrates how individuals' engagement and use of smartphones can be manipulated to inform and strengthen more hierarchical structures of surveillance. Finally, this discussion shows the collapse of traditional boundaries in the digital age with ICTs like smartphones enabling typically private activities to be carried out in

[568] Oxford English Dictionary (7th edn, Oxford University Press, 2012).
[569] Katie Shilton, 'Four billion little brothers? Privacy, mobile phones, and ubiquitous data collection' (2009) 52 Communications of the ACM 48, 48.
[570] Stephen Groening, 'From "a box in the theatre of the world" to "the world as your living room": Cellular phones, television and mobile privatisation' (2010) 12 New Media & Society 1331, 1336.
[571] Hatuka and Toch (n 519) 984.

public (online) space, and vice versa. This section is structured as follows: (i) location-based gaming; (ii) health-tracking; and, (iii) policing and national security.

2.1 Location-based gaming

GPS-enabled smartphones allow users to carry out a range of different activities such as location-based gaming and social networking. Emerging from these location-based activities is 'a new layer to one's digital presentation of self - location.'[572] Accessibility to GPS technology thus enables location to become a dimension of individuals' digital (auto-)biographies. However, in doing so, location data also becomes accessible to third parties, such as corporate and state actors.

There are various different types of location-based activities carried out on smartphones, including: online social networking; dating; gaming; and, tracking health-related activities like: running, swimming, cycling, walking, and sleeping. The following focusses on 'Hybrid Reality Games' ('HRGs') which provide a good example of: (i) individual location sharing; (ii) peer-to-peer surveillance; and, (iii) how data generated from such activities can serve to enhance and inform hierarchical surveillance structures. Many of the points made in relation to HRGs are also applicable to other location-based apps.

HRGs 'employ mobile technologies equipped with internet access and location awareness to create a multi-user game space that occurs simultaneously in physical, digital and represented spaces as denoted by the player's mobility.'[573] Surveillance is a key characteristic of most HRGs, used by players to achieve the goals of the game. For example, in the HRG 'I like Frank,' 'street players' use a 2D map on their smartphone to navigate through the physical landscape of Adelaide, Australia. Street players can be viewed and contacted by online players who play from anywhere in the world. The goal is to locate the fictional character of Frank in a specific location of the

[572] Adriana de Souza e Silva and Jordan Frith, 'Re-narrating the city through the presentation of location' in Jason Fredman (ed) *The mobile story: narrative practices with locative technologies* (2013, Routledge) 35.
[573] Adriana de Souza e Silva and Daniel Sutko, 'Playing life and living play: how hybrid reality games reframe space, play, and the ordinary' (2008) 25 Critical Studies in Media Communication 447, 447.

city via the coordination of street and online players. The street player does not have access to the same information as the online player and so has to trust the latter's direction to 'find Frank.'[574] The game is therefore premised on surveillance. As noted by de Souza e Silva and Sutko, the surveillance in 'I like Frank' is a 'positive quality of the game' as it helps players to 'feel comfortable knowing that they are not alone in the city space,' enabling them to 'form a loose bond or relationship' (albeit with strangers).[575]

However, de Souza e Silva and Sutko also note the more sinister effects of surveillance in HRGs, such as the normalisation of surveillance culture through the desensitisation of players to being watched. The authors note that in relation to government surveillance, games like 'I Like Frank' 'not only appear to make this [surveillance] okay, fun, and normal, but also tell people how to become better surveyors of themselves and others.'[576] Thus, the participatory surveillance characteristic of HRGs can serve to provide a supporting infrastructure to more hierarchical practices by recasting the more sinister properties of surveillance into playful techniques of gaming; consequently, increasing expectations of surveillance and reducing expectations of privacy. This is reminiscent of Lyon's 'alternative-opticon' - the 'panopticommodity' - which depicts the spread of panoptic principles from the architectural prison via softer forms like entertainment.[577]

The surveillant nature of location-based gaming is also seen in the HRG 'Pokémon Go' launched by Niantic in 2016. In Pokémon Go, players are represented on a 3D map of their surroundings via their smartphones. On the map, players can see virtual Pokémon-related objects and must walk around their physical surroundings to engage with them. For example, a Pokémon might be situated in the middle of a park on the player's map who will then have to physically walk to that location in order to 'catch' the virtual object. Whilst there is limited surveillance between players on this HRG,

---

[574] For more information on 'I like Frank' visit <http://www.blasttheory.co.uk/projects/i-like-frank/> accessed 18 July 2017.
[575] De Souza e Silva and Sutko, 'Playing life and living play' (n 573) 456.
[576] Ibid 461.
[577] Discussed in Part 1, section 3.3 of this chapter.

Niantic have fallen under scrutiny for their 'Pokémon Go' privacy policy, which states: 'we may disclose any information about you (or your authorised child) that is in our possession or control to government or law enforcement officials or private parties.'[578] The type of information in the 'possession or control' of Niantic includes geospatial activity which includes where a player has been, for how long, and at what speed they are travelling.[579] The app also requires access to users' cameras and requests permission to access their contact list. Furthermore, the app collects information sent by the smartphone while using the app, such as, 'a device identifier, user settings, and the operating system of your…device.'[580]

In July 2016, Pokémon Go also requested full access to users' Google accounts which included emails, search histories, and Google docs. Although Niantic later claimed that this had been an error and rolled back its privacy permissions accordingly, a vast amount of personal information is still collected by Niantic who can then share it with corporate or state actors.[581] In addition to this, Pokémon Go not only observes where its players are going, but can also dictate where they go via in-game incentives.[582] In Japan, for example, fast food chain 'McDonalds' sponsors the game and, in return, its restaurants provide the locations of over 3000 'Pokémon Gyms' where players go to train their Pokémon. This demonstrates how individuals' locations are both monetised and controlled through the game.[583]

'I like Frank' and 'Pokémon Go,' reveal the extent to which location-based gaming can: (i) directly feed into top-down practices of surveillance, with locations being collected and shared among corporate and state bodies for the purposes of targeted

---

[578] Niantic,'Pokémon Go privacy policy,' s 3(e) <https://www.nianticlabs.com/privacy/pokemongo/en/> accessed 18 July 2017.
[579] ibid s 2(e).
[580] ibid s 2(d).
[581] Olivia Solon, 'Have you given Pokémon Go full access to everything in your Google account?' (*Guardian News*, 12 July 2016) <https://www.theguardian.com/technology/2016/jul/11/pokemon-go-privacy-security-full-access-google-account> accessed 22 June 2018.
[582] NYU Centre for Data Science, 'How is Pokémon Go collecting data on its users' <http://datascience.nyu.edu/how-is-pokemon-go-collecting-data-on-its-users/> accessed 18 July 2017.
[583] Matt Kamen, 'Pokémon Go's first sponsored location will be McDonald's – in Japan' (*Wired*, 2016) <http://www.wired.co.uk/article/pokemon-gos-first-sponsored-location-will-be-mcdonalds-in-japan> accessed 18 July 2017.

advertising or law enforcement; and, (ii) indirectly support vertical architectures of surveillance by normalising players to surveillance, recasting it as a fun and playful activity and inducing self-disclosure. Questions are subsequently raised in relation to players' locational privacy.

On one hand, it could be argued that players voluntarily submit themselves to HRGs; explicitly accepting terms and conditions permitting the sharing of their data and, as such, cannot maintain a reasonable expectation over their locational privacy or other data shared (although, it will not always make good business sense for companies to share customer data and so they will often place limits on the information shared).[584] However, countering this argument is the fact that individuals agree to share their location in order to participate in a game and are not necessarily aware of the extent to which this data is being used to inform other infrastructures of surveillance (despite these being disclosed in (convoluted) terms and conditions).

As established in Chapter 2, acting publically does not eliminate one's expectations of privacy.[585] Rather, more must simply be done by way of surveillance in order to trigger Article 8(1), such as processing information in a manner that is not reasonably foreseeable to the person concerned.[586] Therefore, it is important that laws regulating surveillance do not misconstrue the individual's participation in digital data exchanges as a carte blanche for surveillance, else they risk falling foul of human rights standards by failing to acknowledge reasonable expectations of privacy where necessary. Accordingly, this thesis argues that in order for surveillance laws to fulfil the legality requirements of Article 8 ECHR, they must recognise the technocultural changes that

---

[584] As shown by the *Apple v FBI* case where Apple refused to unlock the iPhone of the San Bernadino shooter on the basis that it would be cost 'significant' time and resources to create a new operating system to do so, and would jeopardise the future security of all Apple devices. The case was filed in the US District of Court for the Central District of California in December 2015 and is captioned 'In the matter of the search of an Apple iPhone seized during the execution of a search warrant on a black Lexus IS300, California License Plate 35KGD203.' For Apple's objections to the request see, 'Notice of objections to February 16, 2016 order compelling Apple Inc. to assist agents in search,' available via <https://www.justsecurity.org/wp-content/uploads/2016/03/FBI-Apple-Apple-Notice-of-Objections.pdf> accessed 17 August 2017.

[585] See discussion of *Peck v UK* (n 23) and *Friedl v Austria* (n 185) in Chapter 2, sections 1.2.1 and 1.2.2.

[586] As in *Peck v UK* (n 23).

the contemporary surveillance landscape has undergone; for example, by understanding the participation of the individual so that reasonable expectations of privacy are recognised and respected. The extent to which this has been achieved by the IP Act is examined in the following chapters.

2.2 Health-tracking apps

Smartphones host a number of health and fitness apps enabling individuals to monitor, record, and share health data. The mobility with which one's health can be monitored has led to these apps being described as tools of 'm-health' ('m' being short for mobility).[587] Health and fitness apps can include: exercise tracking which uses GPS to track and record activities like running or cycling, suggest new routes, and enable you to compete with friends; diet apps where users can keep a calorie diary, store pictures of their meals, and analyse the nutritional content of their food; menstrual cycle diaries; sugar diaries for diabetics; mental health apps that coach the user in meditation, or provide an interface to talk with therapists; sleeping apps that measure how long and well a user has slept; and pregnancy apps that provide information on pregnancy and enable expecting mothers to diarise their pregnancy. There are also apps that act as health promoters by disseminating medical information, such as, the 'WebMD mobile' app which allows individuals to 'Get trusted health information. Whenever. Wherever.'[588] Smartphones have thus enabled typically private, medical information shared between a doctor and patient, to be monitored and analysed by the individual - and even shared with his or her peers for comparison. Health-tracking on smartphones thus illustrates the fluidity of the public-private boundary brought about the proliferation of this ICT.

Sharon argues that 'the advent of inexpensive digital self-tracking tools, which have made the collection and analysis of data easier, more precise, and more entertaining,

[587] See, Deborah Lupton, 'M-health and health promotion: the digital cyborg and surveillance society' (2012) 10 Social Theory & Health 229, 230.
[588] WebMD app < http://www.webmd.com/mobile> accessed 19 July 2017.

has led to a dizzying rise in the phenomenon of self-tracking for health.'[589] With this 'dizzying rise' has come an unprecedented opportunity for a range of actors to monitor, measure, record and scrutinise users' bodies. In turn, this has led to the conceptualisation of health-tracking apps as surveillance, particularly in terms of first and second wave surveillance with scholars invoking the works of Foucault, Deleuze, and Haggerty and Ericsson.

Lupton, for example, notes that 'the emergence of m-health potentially reconfigures the subject of surveillance and complicates the concept of the panoptic gaze' on the basis that: 'While there still may be an expert exerting the panoptic gaze upon the individual…these technologies also encourage users to turn the gaze upon themselves or to actually invite others to do so.'[590] To illustrate this, Lupton notes the convergence of health apps and social networking sites to allow users to share their health data with their social media followers who are 'invited to contribute by the user to monitor their bodily habits.'[591] Thus, not only are individuals responsibilised through these apps to surveil their own health care and management, they are also integrated into a 'heterogeneous network of actants, which include the various technologies employed but also friends and contacts.'[592] Such a criss-crossing of the gaze leads Lupton, alongside other scholars, to employ Haggerty and Ericson's concept of the 'surveillant assemblage' to better capture the convergence of the body and technology through the notion of the 'flesh-technology hybrid.'[593] However, upon the creation of a data-double in the surveillant assemblage, Lupton argues that health apps do not decorporealise the body as data is fed back to the individual to encourage self-scrutinisation and enable them to adapt their lifestyle accordingly.[594] In this sense, Deleuze's 'society of control' becomes more relevant as 'self-care and self-

[589] Tamar Sharon, 'Self-tracking for health and the quantitative self: re-articulating autonomy, solidarity, and authenticity, in an age of personalised healthcare' (2017) 30 Philosophy & Technology 93, 96.
[590] Lupton (n 587) 236.
[591] Ibid 236.
[592] Ibid 237.
[593] Haggerty and Ericsson (n 362) 611. See Part 1, section 2.1 of this chapter.
[594] Lupton (n 587) 237.

improvement…"seep out" of their disciplinary confines' [– and –] 'become matters of concern for the space and time *adjoining* institutional sites.'[595]

The above positioning of health apps as part of surveillance culture highlights the potentially disempowering consequences of self-tracking 'insofar as it invites an increased control of others – health promoters, friends, and followers, and even the internalised health promoter of one's own super ego – over oneself.'[596] However, the participatory nature of individuals' engagement with such apps ought also to be acknowledged as

> 'individuals are not coerced into providing information or downloading health-related apps…They do so voluntarily and willingly in order to improve their health or physical fitness, reduce their consumption of alcohol, give up smoking or lose weight.'[597]

This is supported by the 'Quantified Self' movement founded as a website in 2007 where self-tracking enthusiasts could discuss their experiences and findings.[598] In explaining the movement, co-founder Gary Wolf argues:

> 'When we quantify ourselves, there isn't the imperative to see through our daily existence into a truth buried at a deeper level. Instead, the self of our most trivial thoughts and actions, the self that, without technical help, we might barely notice or recall, is understood as the self we ought to get to know.'[599]

Thus, advocates of the 'Quantified Self' view self-tracking as a self-empowering practice that furthers autonomy and knowledge about one's true self. However, the

---

[595] As noted by Brad Millinton, 'Smartphone apps and mobile privatisation of health and fitness' (2014) 31 Critical Studies in Media Communication 479, 482.
[596] Sharon (n 589), 99.
[597] Lupton (n 587), 245.
[598] Refer to the Quantified Self website, 'Quantified Self: self knowledge through numbers' at <http://quantifiedself.com> accessed 21 July 2017.
[599] Gary Wolf, 'Know thyself: tracking every facet of life, from sleep to mood to pain 24/7/365' (*Wired*, 22 June 2007) <https://link.springer.com/content/pdf/10.1007%2Fs13347-016-0215-5.pdf> accessed 20 July 2017.

movement is criticised in the literature for having a reductionist effect on highly complex human experiences and emotions that are not amenable to numerical translation, such as 'wellness' and 'happiness.'[600] The risk, warns Andrejevic, is that numbers and algorithms are not objective as they are shaped by embedded value judgements.[601] Consequently, self-tracking health apps may be viewed as enforcers of predetermined norms and as mechanisms of control to ensure conformity with these standards. Furthermore, personal data generated through these apps can be used by various different actors in unforeseeable ways. For example, although mobile self-tracking can help the individual to manage their own health, it can also function as an actuarial tool by acting as a live medical report that puts users at risk of sanction or discrimination by organisations.[602] This is demonstrated by the inclusion of health-tracker data by some employers in 'wellness programs' whereby lower insurance premiums are offered to employees with a higher number of steps taken.[603] 'Fitbit'[604] data has also been used in the law enforcement context as evidence in personal injury and criminal cases across the US and Canada.[605] Therefore, despite health-tracking data being used by the individual for self-improvement and self-actualisation, its creation of a 'digital identity' can simultaneously facilitate the exclusion of 'certain individuals and groups from access to goods and services or to identify them as security risks.'[606]

Whilst the individual actively participates in the creation and sharing of data about his or her health via health-tracking apps, as argued by the 'Quantified Self' movement this is undertaken for the purposes of self-care and even empowerment. The

---

[600] Sharon (n 589) 261.
[601] See Mark Andrejevic, 'The big data divide' (2014) 8 International Journal of Communications 1673.
[602] See Martin French and Gavin Smith, '"Health" surveillance: new modes of monitoring bodies, populations, and polities' (2013) 23 Critical Public Health 383, 388.
[603] As shown in a study carried out by ABI Research, 'Corporate wellness is a 13 million unit wearable wireless device opportunity' (*ABI Research*, 25 September 2013) <https://www.abiresearch.com/press/corporate-wellness-is-a-13-million-unit-wearable-w/> accessed 24 July 2017.
[604] A wearable health technology that synchronises with the user's smartphone.
[605] See Samuel Gibbs, 'Court sets legal precedent with evidence from Fitbit health tracker,' (*The Guardian*, 18 November 2014) <https://www.theguardian.com/technology/2014/nov/18/court-accepts-data-fitbit-health-tracker> accessed 24 July 2017.
[606] Sharon (n 589) 261.

subsequent manipulation of this data for disciplinary or controlling purposes thus threatens these benefits bestowed on civil society by the democratisation of surveillance in the digital age. Thus, similar to the conclusion reached in relation to 'location-based gaming' above, it is important that the law recognises individuals' ownership of digital data exchanges so that their participation in surveillance culture (and the benefits that flow from this) is protected and not undermined. The law must not falsely assume that expectations of privacy are sacrificed upon the individual's engagement in these practices, else risk the unjustified extension of the hierarchical gaze which not only threatens privacy, but so too the benefits emerging from individuals' participation in surveillance culture. In light of this, the positioning of participation under the IP Act is established in the following chapter and its impact on the protection of privacy is critically assessed under Article 8 ECHR in Chapter 5.

2.3 Policing and national security: Snowden, Smurfs, and smartphones

2.3.1 The individual - a dutiful flâneur

Smartphones enable individuals to actively contribute to and participate in state surveillance practices. Larsson describes citizens as the 'first line of defence,' as they are increasingly responsibilised to carry out everyday surveillance and report to authorities on activities or persons that are 'unusual' or 'suspicious.'[607] To illustrate this responsibilisation of the individual, Larsson adopts Benjamin's figure of the 'flâneur' derived from the French 'flânerie,' meaning 'to stroll.' The flâneur is an urban dweller who strolls aimlessly, observing the public spaces of an emerging city. He is described as 'an amateur detective' and as

> 'an optical rather than tactile agent, a curious and autonomous agent of surveillance who hides within crowds in the streets, keenly gathering the visual data emerging before its eyes and filtering it through lived experiences.'[608]

[607] Sebastian Larsson, 'A first line of defence? Vigilant surveillance, participatory policing, and the reporting of "suspicious" activity' (2016) 15 Surveillance & Society 94.
[608] Walter Benjamin, *The Arcades Project* (Cambridge University Press, 2002), 417; Larsson ibid 96.

The flâneur was initially an amateur detective out of pleasure, however, Larsson argues that today the figure is

> 'confronted with expectations of what it entails to be a "good" citizen. Its eyes and ears become political participants and serve as extensions and embodiments of security institutions.'[609]

Larsson uses this concept of the contemporary flâneur to argue that citizens who might previously have watched for fun or enjoyment as virtue of their own freedom, are now increasingly placed under a duty to record and report any 'suspicions' - 'to participate in the so-called war on terror from the privacy of their homes, from their workplaces, and during their spare time.'[610] This is made possible by the democratisation of (surveillance) power via ICTs (like smartphones) that enable the individual to record and share anything they deem 'suspicious.' During the London 2011 riots, for example, the police used an app called 'FaceWatch' that enabled smartphone users to view police photos and contact police if they recognised someone – like a digital line-up.[611]

Smartphones thus bridge the gap between the contemporary dutiful flâneur on the ground and the central authorities by enabling instantaneous reporting of 'signs or shades of terror yet to come.'[612] In this sense, they can be described as 'technologies of citizenship' [– that -] 'foster the capacities for active participation' and enable an offloading of duties onto the citizenry,[613] ultimately providing the state with 'a way of governing without governing society.'[614]

However, as shown in the previous sections, smartphones are not always used *by* the individual; they also facilitate an extension of the state's gaze discreetly and

---

[609] Larsson (n 607) 97.
[610] Ibid 98.
[611] See, *BBC News*, 'Crowd-sourcing used to trace London riot suspects' (*BBC News online,* 26 June 2012) <http://www.bbc.co.uk/news/uk-england-london-18589273> accessed 2 August 2017.
[612] Larsson (n 227) 103.
[613] Mitchell Dean, *Governmentality: power and rule in modern society* (2nd edn, 2010, Sage publishing) 222.
[614] Ibid.

ubiquitously across society. This was highlighted by Snowden's exposure of the vast number of tools used by state intelligence agencies to glean communications content and data from smartphones. According to an internal NSA document entitled 'Exploring current trends, targets, and techniques,' the proliferation of smartphones was happening 'extremely rapidly' and complicating traditional target analysis.[615] An internal GCHQ document also stated that the agency was not only interested in collecting voice, SMS, and geo-location data but also 'getting intelligence from all the extra-functionality that iPhones and Blackberry's offer.'[616] Snowden thus revealed just how aggressively surveillance tools were developed in order to fulfil this desire.

2.3.2 The 'Smurf suite'

GCHQ developed a malware toolkit called 'Smurf suite' that allowed UK intelligence agencies to hack into smartphones. There are various different 'Smurfs' that enable different types of smartphone surveillance, for example: 'Nosey Smurf' can switch on the microphone of a smartphone; 'Tracker Smurf' is a geolocation tool that facilitates high-precision tracking; 'Dreamy Smurf' allows a phone to be switched on or off remotely, and; 'Paranoid Smurf' conceals the operation of other Smurfs from the eyes of, say, phone technicians.[617] The NSA also developed other tools that were subsequently used by GCHQ, including: 'GUMFISH' which enables agents to take photographs via an individual's smartphone; 'FOGGYBOTTOM' which stores passwords typed into internet browsers; and, 'GROK' which stores keystrokes.[618]

It is uncertain exactly how widely the above tools were implemented. However, in a case brought by NGO 'Privacy International' against GCHQ at the Investigatory Powers Tribunal ('IPT'), it was held that the government had the power to hack

---

[615] See, Marcel Rosenbach, Laura Poitras, Holger Stark, 'How the NSA accesses smartphone data' (*Spiegel online*, 9 September 2013) <http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html> accessed 2 August 2017.
[616] Nick Hopkins, Julian Borger, Luke Harding, 'GCHQ: Inside the top secret world of Britain's biggest spy agency' (*The Guardian*, 2 August 2013) <https://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden> accessed 26 July 2017.
[617] For information on the 'Smurf suite' see Anderson (n 158) para 15.
[618] See Ryan Gallagher and Glenn Greenwald, 'How the USA plans to infect "million" of computers with malware' (*The Intercept*, 12 March 2014) < https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/> accessed 2 August 2017.

devices pursuant to the Intelligence Services Act 1994.[619] Under the Act, the above types of equipment interference were deemed lawful following a 'thematic warrant' (general warrants covering a class of property, persons, or conduct).[620] As noted in the case, such warrants might reasonably include 'all mobile phones in Birmingham,' and so it is reasonable to conclude that large numbers of devices were subject to these practices.[621]

The Snowden disclosures also revealed the extent to which phone providers co-operated with intelligence agencies under the 'Tempora' programme. 'Tempora' is effectively the British version of 'PRISM' that involves tapping into undersea fibre-optic cables to access telephone and internet traffic.[622] The program was implemented with the help of phone providers (including 'BT' and 'Vodafone') who provided unlimited access to data passing along their cables.[623] This meant that customers' phone calls, text messages, emails, and social media activity became accessible to GCHQ. Subsequent to collection, the data was filtered by the NSA and GCHQ intelligence agents via the use of search terms.[624] Whilst companies were required to co-operate with government requests under the Telecommunications Act 1984,[625] Eric King Deputy (Director of NGO 'Privacy International') questions whether companies were strong-armed into co-operating or went beyond the requirements of law and acted as voluntary intercept partners.[626] The partnership between these private actors and the state illustrates the interconnectedness of surveillance hierarchies in the contemporary

---

[619] Intelligence Services Act 1994, s 5.
[620] *Privacy International v Secretary of state for foreign and commonwealth affairs and GCHQ* [2016] UKIP Trib 14_85-CH. Further discussion on 'thematic warrants' in Chapter 4, Part 2, section 1.3.
[621] *Privacy International v Secretary of state for foreign and commonwealth affairs and GCHQ*, ibid, [36].
[622] For the 'Tempora' PowerPoint slide released by Snowden see, Guardian News, 'NSA PRISM program slides' (*Guardian news*, 1 November 2013) <https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document> accessed 22 June 2018.
[623] See James Ball, Luke Harding and Juliette Garside, 'BT and Vodafone among telecoms companies passing details to GCHQ' (*Guardian news*, 2 August 2013) <https://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq> accessed 31 July 2017.
[624] Reportedly 40,000 search terms used by GCHQ and another 31,000 used by the NSA according to Privacy International, 'Eyes wide open: special report' (Version 1.0, *Privacy International*, 26 November 2013) <https://www.privacyinternational.org/node/301> accessed 27 July 2017, at 13.
[625] Telecommunications Act 1984, s 94.
[626] James Ball et al (n 623).

landscape and the extent to which individuals' smartphone usage has facilitated an extension of the state (and corporate) gaze. The extent to which this relationship between state and corporation has been strengthened by the IP Act (which places legal obligations on service providers to assist in the implementation of warrants) is demonstrated in Chapter 4.

The above demonstrates that whilst smartphones enable individuals to actively participate in the vertical axis of surveillance by offering information *up* to authorities, they have also facilitated mass state surveillance practices which pose serious risks to privacy. As established in Chapter 2, the law must provide sufficient clarity as to circumstances in which public authorities are permitted to resort to surveillance practices. However, the very nature of thematic powers runs contrary to this requirement as they are framed generally to include types of persons, conduct, or areas, rather than specific targets. Thus, it is highly questionable whether persons are provided with 'sufficient clarity' as to the circumstances in which they might be subjected to such 'thematic' surveillance.

Whilst the previous legal framework allowing for the above types of surveillance in the UK has been replaced by the IP Act, thematic warrants and bulk surveillance powers continue feature in the new legislation. These powers are examined in the following chapter to establish the IP Act's approach to the contemporary surveillance landscape, particularly its approach to the participation of the individual. Chapter 5 subsequently examines this approach in terms of its impact on privacy via an analysis of such 'bulky' surveillance powers under Article 8 ECHR. This enables a conclusion to be reached as to the suitability of UK surveillance law in terms of its protection of privacy in the digital age.

2.4 Summary

The above analysis of smartphones as a site of third wave surveillance has illustrated the reality of the third wave landscape where there exists a hybrid of actors and functions of surveillance. As Galic et al note, 'the perception of the surveillant gaze is in the eye of the beholder' and within the third wave landscape, there are many

beholders for the law to now consider.[627] This section also demonstrates that the non-vertical and vertical axes of surveillance are not always working against each other, with individuals using technology to actively participate in state surveillance practices. However, as revealed by Snowden, smartphones have also enabled the state and corporation to extend their surveillant gaze without the consent or knowledge of the individual. Camacho notes:

> 'No one disputes that individuals use cell phones to share vast amounts of personal information with third parties voluntarily. While individuals choose to share this information, it is the transactional and location data, material unconsciously shared, that may provide the most intimate portrait of a person's identity.'[628]

Thus, whilst smartphones can be used by individuals to carry out types of participatory surveillance (eg peer-to-peer, autobiographical, and sousveillance) the popularity and multi-functionality of this ICT has also enabled first and second wave surveillance practices to thrive. Therefore, whilst there is a need to go beyond the Panopticon and surveillant assemblage in order to recognise the additional actorship of the individual, Snowden reveals the extent to which traditional conceptions of surveillance retain relevancy in the contemporary surveillance landscape.[629] This is supported by an NSA PowerPoint slide which states:

> 'Who knew in 1984 that this [in reference to an image of Apple founder, Steve Jobbs] would be Big Brother and the zombies [in reference to an image of Apple customers] would be paying customers?'[630]

---

[627] Galic et al in Brownsword et al (n 64), 747.
[628] Sean Camacho, 'Can you hear me now? Time to consider whether cell phone providers are state actors' (2016) 49 Suffolk University Law Review 257, 279.
[629] This is supported by Lyon who notes that disciplinary theories of surveillance have not been superseded but are inadequate on their own, see David Lyon, 'Surveillance, power, and everyday life' in Chrisanthi Avegerou, Robin Mansell, Danny Quah, Roger Silverstone (eds) *The Oxford handbook of information and communication technologies* (Oxford University Press, 2009) 452.
[630] See Rosenbach et al (n 615).

Thus, offsetting the benefits of participatory surveillance facilitated by smartphones, is the ability of the state (and corporation) to simultaneously construct its own identities and assumptions about the individual without his/her consent or knowledge. This information can subsequently form the basis of decisions to exclude, discriminate, discipline and control the individual. Therefore, it is important that laws regulating surveillance recognise the technocultural realities of the digital age not only to protect privacy, but so too, to safeguard the individual's enjoyment of surveillance as an apparatus for sociality, self-care, and empowerment.

Conclusion

By adopting the structure of 'waves of surveillance,' this chapter has illustrated the hybrid and dynamic nature of the contemporary surveillance landscape brought about the digitalisation of society. The disciplinary and controlling functions of first and second wave surveillance provided the foundation for the third wave which builds on, as opposed to supplants, these earlier conceptions of surveillance.

The examination of social media and smartphones as sites of third wave surveillance in Part 2 demonstrates the reality of the third wave surveillance landscape and the legal implications that flow from it. These sites showcased the additional actorship of the individual and the benefits of this democratisation of surveillance power in the digital age (eg sociality, self-care, and empowerment). However, it was also demonstrated how these sites of third wave surveillance can work to enhance and extend more formal structures of surveillance by transcribing into the digital what was previously unrecordable and, therefore, untrackable. In turn, this shows how the non-vertical axis of surveillance can provide something of a supporting infrastructure to the vertical axis of surveillance. In light of this, it was argued that the law must properly position the participation of the individual so that the institutional gaze is not extended to such an extent that it: (i) poses a threat to the personal privacy of individuals; and, (ii) undermines the benefits bestowed on civil society by the contemporary surveillance landscape.

The sites of third wave surveillance also served to illustrate the collapse of traditional boundaries (namely the public-private dichotomy) and the subsequent need for these

to be reconsidered so that privacy can be preserved within the digital age. As shown above, technology is increasingly transferring in-house activities and objects outwith the home and into (virtual) public space. Smartphones, for example, enable individuals to carry and access traditionally home-based items like photographs, videos, documents and communications wherever they go. Similarly, social media has re-located typically private conversations, images and videos from intimate settings to a much more public forum where they can be seen and commented on by other users. Thus, like hermit crabs we now carry our homes around with us – albeit in our pockets and not our backs. This evaporation of the home is also seen with the advent of the 'Internet of Things' ('IoT') which 'comprises an evolving array of technologies that extend the idea of instantaneous connectivity beyond computers, smartphones, and tablets to everyday objects such as home appliances, cars, and medical devices.'[631] Despite these developments, the following chapter demonstrates a rigid attachment to the public-private dichotomy under the IP Act (alongside other increasingly outdated distinctions) and the consequences this has for the protection of personal privacy in the digital age. This is used to support the core argument of this thesis that the IP Act fails to attune to the technocultural realities of the contemporary surveillance landscape.

Finally, the sites of third wave surveillance have shown how the explosion of personal data traffic in the digital age has facilitated an extension of the surveillant gaze over *everyone* as opposed to just *someone*. The following chapter demonstrates that whilst not all of the information gathered may be personal or private, its aggregation into vast databases and analysis via Big Data techniques seriously threatens the societal value of privacy discussed in the Introduction to this thesis. However, as established in Chapter 2, there is limited scope for the realisation of privacy on a group level under Article 8 ECHR. The following chapter underlines the need for the development of such a right by demonstrating the extent to which the bulk, data-focussed powers listed

[631] Swaroop Poudel, 'Internet of things: underlying technologies, interoperability, and threats to privacy and security' (2016) 31 Berkeley Technology Law Journal 997, 998.

under the IP Act pose a general, collective harm as opposed to the type of concrete, personal harm that is typical of Article 8 claims against surveillance.

Chapter 4 The UK surveillance legal landscape

Introduction

This chapter establishes the UK's approach to the contemporary surveillance landscape via an analysis of the IP Act's response to the legal implications of the third wave identified in Chapter 3.

Discussion is divided into two parts. Part 1 provides an overview of the current UK surveillance legal landscape. The law in this area is vast and has undergone significant change over the past two years. It is further complicated by recent reform of European data protection law. Part 1 thus serves to contextualise subsequent discussion. Part 2 goes on to examine the IP Act's approach to the contemporary surveillance landscape, focussing on aspects of the Act that are illustrative of its response to the legal implications flowing from the third wave. These were identified in Chapter 3 as follows: (i) the collapse of traditional dichotomies; (ii) the participation of the individual; and, (iii) the need for group privacy.

Based on this discussion, it is concluded that the IP Act has struggled to respond to the technocultural reality of the contemporary surveillance landscape. The impact of this is subsequently examined in terms of the Act's protection of privacy in Chapter 5. This chapter therefore contributes to the core argument of this thesis - that UK surveillance law does not adequately protect privacy in the digital age as it fails to recognise the technocultural changes that the contemporary surveillance landscape has undergone. Recommendations as to how this might be remedied are provided in Chapter 6.

Part 1 The UK surveillance legal landscape: an overview

The Draft Investigatory Powers Bill ('IP Bill') was introduced by the Home Office in November 2015 in response to the legal fallout from the Snowden disclosures and following three major reports from: the Government's Independent Reviewer of Terrorism Legislation;[632] The Royal United Services Institute ('RUSI');[633] and, the

[632] Anderson, *A question of trust* (n 158).
[633] RUSI report (n 58).

Intelligence and Security Committee ('ISC').[634] Whilst the recommendations of each differ to some extent, they agreed that the existing surveillance legal framework was outdated, unnecessarily complex, lacked transparency and should be replaced by a new law consolidating existing surveillance powers.[635] Each also stressed the importance of greater judicial oversight in the authorisation of warrants.[636]

Following pre-legislative scrutiny by the Joint Committee on the Draft IP Bill and the Joint Committee on Human Rights, the bill received Royal Assent on 25 November 2016 and is now the primary law governing the investigatory powers of security and intelligence agencies ('SIAs') and law enforcement agencies ('LEAs'), although as shown below, some surveillance powers remain under pre-existing legislation. Some parts of the IP Act have also yet to come into force.[637]

Prior to the IP Act coming into force, surveillance practices were covered by an array of different laws, although primarily under RIPA which governed SIA and LEA powers to intercept communications and acquire communications data. RIPA was passed in response to the enactment of the Human Rights Act in 1998 and the *Halford v UK* case in 1997 where it was held that the interception of communications on private networks was not in accordance with law under Article 8 ECHR.[638] Since its inception, RIPA has been criticised for being overly complex, inaccessible, and lacking in adequate safeguards against abuse.[639] Such criticism grew alongside technological developments exposing lacunae in the law's protection which posed serious risks to privacy.

---

[634] ISC, *Privacy and security: a modern and transparent legal framework* (2014-15, HC 1075).
[635] Anderson's report and and the RUSI report agreed only RIPA Part 1, DRIPA 2014, and CTSA Part 3 should be consolidated under one law whereas the ISC report recommended that all laws relating to intelligence agencies be combined into a single legal framework.
[636] Anderson especially stressed the importance of judicial oversight, advocating the creation of an Independent Surveillance and Intelligence Commission ('ISIC') consisting of a Chief Commissioner, a body of Judicial Commissioners, and an Inspectorate (Anderson Report (n 158) Recommendation 22).
[637] For example, the bulk powers are yet to come into force.
[638] *Halford v UK* (n 197).
[639] Gabrielle Garton Grimwood and Christopher Barclay, *The Regulation of Powers Bill: Bill 66 of 1999-2000* (2000, House of Commons Research Paper 00/25) 63-65. See Chapter 2, section 2.1.1, at n 257.

As mentioned above, RIPA was part of a complex framework of laws governing surveillance. For example, interception powers were also covered under: The Wireless Telegraphy Act 2006; the Telecommunications Act 1984; PACE 1984; the Terrorism Act 2000; and Part 11 of ATCSA 2001 (some of which have been touched on in previous chapters). The Intelligence Services Act 2004 also provided the Secretary of State with the power to issue warrants, authorising SIAs to interfere with property and, as most recently avowed by government, to carry out 'Computer Network Interference' ('CNE') (also described as 'hacking').[640] The Police Act 1997 granted similar powers to LEAs. Furthermore, RIPA only covered the acquisition and disclosure of data, leaving the retention of data to be dealt with separately under the Data Retention Regulations 2009 which transposed the EU Data Retention Directive ('DRD') of 2005 into domestic law. This was later replaced by DRIPA 2014 following the CJEU's invalidation of the Data Retention Regulations in the *DRI* case (discussed below).[641]

Whilst there were challenges to the UK's surveillance law framework before Snowden,[642] the disclosures highlighted the true extent of the fragmented, complex, and non-transparent system of laws being used to permit mass surveillance of communications across the UK. Thus, the Snowden disclosures can be viewed as the 'final nail in the coffin' for the prior system of laws governing state surveillance in the UK.

Despite the aim of the IP Act to 'bring together all of the powers already available to SIAs and LEAs to obtain communications and data about communications,' not all powers have been incorporated under the Act.[643] 'Digital' and 'real world' investigations continue to be dealt with separately. The latter (eg covert human

---

[640] Avowed in Home Office, *Equipment interference: draft code of practice* (Crown Publishing, 2016), para 2.6.
[641] *DRI* (n 15). Council Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54 (Data Retention Directive).
[642] *Liberty and ors v UK* (2009) (n 167).
[643] Secretary of State for the Home Department, *Investigatory powers bill: government response to pre-legislative scrutiny* (Cm 9219, 2016), para 7.

intelligence sources ('CHIS')) remains under RIPA and the former (eg interception, data acquisition, equipment interference) falls under the IP Act. Several of the powers in the IP Act have also been criticised for being unnecessarily broad and ill-defined, failing to provide the general public with a comprehensive understanding of its powers and when they can be used. This conclusion is also reached in the following chapter following a critical examination of the IP Act's thematic and bulk surveillance powers under Article 8 ECHR. Whilst the justification behind the breadth of terms in the Act is the protection of national security - as overly explicit provisions threaten to undermine the very nature and logic of secret surveillance - critics maintain that the law is excessively fastidious in this regard and to the detriment of individuals' privacy.[644]

Outwith the UK, there have also been significant changes at a European level with the reform of EU data protection law. Most notably, the 'General Data Protection Regulation' ('GDPR')[645] replaces the previous EU 'Data Protection Directive.'[646] The GDPR is aimed at 'strengthening citizens' fundamental rights in the digital age and facilitating business by simplifying rules for companies in the Digital Single Market.'[647] Despite the UK's impending departure from the EU, the GDPR was brought into force in the UK on 25 May 2018 via the Data Protection Act 2018 and the government has stated it will continue to adhere to these standards post-Brexit.[648]

The GDPR applies to organisations that process data in the EU and organisations based outwith the EU who offer goods and services to Member States.[649] The GDPR applies

---

[644] As noted by Big Brother Watch in its written evidence to the Joint Committee on the Draft IP Bill (DIP0007) <https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf> accessed 18 October 2017, at 158
[645] Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (GDPR).
[646] Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJL281/31 (Data Protection Directive).
[647] European Commission Fact Sheet, 'Questions and answers – data protection reform package' (24 May 2017) <http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm> accessed 31 October 2017.
[648] Prime Minister's Office, 'The Queen's Speech 2017' (21 June 2017) <https://www.gov.uk/government/speeches/queens-speech-2017> accessed 14 August 2018.
[649] GDPR, art 3.

only to 'personal data' which includes, 'any information relating to an identified or identifiable natural person ('data subject').'[650] The definition of this phrase has been expanded from the Data Protection Directive to reflect changes in the technological landscape and the increased collection of data about persons by organisations.[651] Accordingly, the definition now includes a wide range of personal identifiers to constitute personal data, including: name, identification number, location data or online identifier, such as an IP address - a unique code that identifies a device connected to the Internet or a local network.[652] Some other key changes include: stronger requirements for consent;[653] greater extra-territorial scope;[654] the introduction of penalties including administrative fines;[655] notification requirements;[656] a strengthened right to be forgotten;[657] and the incorporation of data protection by design.[658] The regulation does not apply to activities relating to national security which falls outside the scope of EU law.[659] Processing for law enforcement purposes is now covered under the 'Police and Criminal Justice Directive'[660] (commonly referred to as the 'Law Enforcement Directive') which came into force this year and aims to

> 'facilitate a smoother exchange of information between Member States' police and judicial authorities, improving cooperation in the fight against terrorism and other serious crime in Europe.'[661]

---

[650] Ibid, art 4.
[651] Information Commissioner's Office, 'Key definitions' (*ICO*) <www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/.> accessed 24 June 2018.
[652] Ibid, art 4.
[653] GDPR, ss 32-33.
[654] Ibid, art 3.
[655] Ibid, ss 148-153.
[656] Ibid, art 19.
[657] Ibid, art 17.
[658] Ibid, art 25.
[659] Ibid, s 16.
[660] Council Directive 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (Law Enforcement Directive).
[661] European Commission Fact Sheet (n 647).

Whilst only some aspects of the above laws will be touched on in this chapter due to limited word count and relevance, it suffices to show for now the evolution of the European landscape within which the domestic system is situated.

Having provided an overview of the current UK surveillance legal landscape, Part 2 goes on to examine the UK's legal response to the contemporary, third wave surveillance landscape.

Part 2 The UK approach to the third wave

This part establishes the UK's approach to the contemporary surveillance landscape via an analysis of the IP Act's response to the legal implications of the third wave identified in Chapter 3: (i) collapsing dichotomies; (ii) the participation of the individual; and, (iii) the need for group privacy. With regard to the third implication, discussion is centred more around the *impact* of the IP Act on group privacy rather than the Act's recognition of such a right. As established in Chapter 2, limited scope for group privacy currently exists under Article 8 ECHR and so this discussion is used to underline the need for the development of such a right in the digital age.[662]

Having established the IP Act's approach to the third wave landscape a conclusion is reached as to the suitability of UK surveillance law in the digital age in terms of its impact on privacy. This conclusion is then supported by an analysis of the IP Act under Article 8 ECHR in Chapter 5.

1 Collapsing dichotomies

The examination of smartphones and social media in Chapter 3 demonstrated the collapse of traditional boundaries in the digital age, particularly that of the public-private dichotomy. Given that laws are formed according to such 'boundary-marking concepts' it is important that when these boundaries converge or change, the law adapts accordingly so that it remains relevant, coherent, and effective.[663]

---

[662] See further Chapter 2, section 4.
[663] See discussion of collapsing dichotomies in Chapter 3, Part 2 (section 1.3.2 deals specifically with dangers of maintaining the public-private dichotomy in the digital age).

This section examines the extent to which the IP Act has adapted to the collapse of dichotomies in the digital age. This is achieved via an examination of three distinctions maintained in the IP Act: (i) 'domestic' and 'overseas;' (ii) 'content' and 'data;' and, (iii) 'bulk' and 'targeted.' It is demonstrated how technology has blurred previously distinct concepts and the risks to privacy arising from the law's failure to acknowledge such convergence in the digital age. From an analysis of the IP Act's distinction between 'content' and 'data,' higher level conclusions are also made as to the IP Act's approach to the public-private dichotomy. The impact of this distinction on the protection of privacy is then critically assessed in terms of Article 8 ECHR in Chapter 5.

1.1 'Domestic' vs. 'overseas'

The IP Act grants the intelligence and security agencies with three types of 'bulk' surveillance powers enabling the mass surveillance of communications: bulk interception; bulk acquisition of communications data and personal datasets; and, bulk equipment interference ('EI') ('EI' refers to the interference with any equipment for the purpose of obtaining communications, equipment data, or any other information).[664] Whilst critics argue that these powers did not exist in law prior to the IP Act,[665] the government maintains that they were exercised under: RIPA 2000; the Telecommunications Act 1984; and, the Intelligence Services Act 1994. As recommended by the RUSI, Anderson, and ISC reports, the IP Act consolidates these powers into a single legal framework.[666] Whilst the bulk powers of the IP Act will be examined in more detail below, this section examines the inherent distinction between 'domestic' and 'overseas' underlying the bulk interception power.[667]

The IP Act states that the main purpose of bulk interception is 'the interception of overseas-related communications.'[668] 'Overseas-related communications' are defined

---

[664] IP Act 2016, part 6. For definition of EI see, ss 99 and 176. For definition of 'equipment data' see, ss 100 and 177.
[665] Matthew Ryder QC describes the bulk powers as 'essentially new,' in 'Oral Evidence to the Draft Investigatory Powers Bill' (2015, HC651), Q186.
[666] Anderson (n 158), RUSI (n 58), ISC (n 634).
[667] IP Act, s 136.
[668] IP Act, s 136(2)(a).

as communications sent or received by individuals outside the British Islands.[669] Therefore, this definition functions on a distinction between 'domestic' and 'overseas' communications in order to (theoretically) exclude the former from the bulk surveillance regime. However, this distinction is a difficult one to maintain in the digital age where the 'global nature of the internet' means that even domestic communications are often routed outside the UK.[670] This fact led the Joint Committee on the Draft IP Bill to conclude that the 'limitation of the bulk powers to "overseas-related" communications may make little difference in practice to the data that could be gathered under these powers.'[671]

The conclusion of the Joint Committee on the Draft IP Bill is supported by proceedings brought before the Investigatory Powers Tribunal ('IPT') in 2014 by a group of NGOs challenging the legality of programs exposed by Snowden, such as PRISM and Tempora.[672] The case revealed that the government functions on a very broad definition of 'external communications' that included interactions with foreign internet servers.[673] Consequently, individuals' engagement with sites like Facebook, Google, and Twitter can constitute 'overseas' communications, even when accessed domestically, due to the servers of these sites being located outside the British Islands. This is also the case for documents stored on cloud-based servers outwith the UK.

It was also shown that under the Tempora program, domestic communications were incidentally swept up due to bulk interception being achieved via the tapping of fibre-optic cables through which a colossal amount of internet traffic flows.[674] The IP Act *does*, however, provide a safeguard for domestic communications that have been acquired incidentally under a bulk interception warrant by requiring a targeted warrant for its examination.[675] This demonstrates at least *some* awareness of the fragility of the

---

[669] Ibid, s 136(3).
[670] Joint Committee on the Draft Investigatory Powers Bill, *Legislative scrutiny: Draft Investigatory Powers Bill* (2016, HL 93, HC 651), para 323.
[671] Ibid.
[672] *Liberty and others v GCHQ* [2014] UKIPTrib 13_77-H. PRISM and Tempora covered in Chapter 3, Part 2, section 1.3.2.3.
[673] *Liberty v GCHQ*, ibid, [97]. Also confirmed in the ISC report (n 634) para 109.
[674] *Liberty v GCHQ* (n 672), [78].
[675] IP Act, s 15(3).

domestic-overseas dichotomy by the IP Act.[676] However, the effectiveness of this additional safeguard is undermined by the lack of an equivalent safeguard for the retention and examination of domestic communications *data* which, as shown in section 1.2 below, can be equally if not more revealing than the *content* of a communication.

The above distinction between 'domestic' and 'overseas' emphasises the failure of the IP Act to appreciate the collapse of traditional dichotomies in the digital age by failing to appreciate the global nature of individuals' interactions online – even between individuals based in the UK. The Act's maintenance of a false dichotomy between 'domestic' and 'overseas' communications means that UK-based electronic communications (eg email or social media messages) are failing to receive the same protection afforded to their analogue equivalents (eg letters or landline telephone calls). In light of the extent to which individuals now communicate digitally, this distinction represents a significant weakness in the IP Act's protection of privacy in the digital age.

1.2 'Content' vs. 'data'

The Anderson report recommended that definitions for 'communications content' and 'communications data' be included in the new legal framework and that they be developed in light of input from service providers, tech experts, and NGOs.[677] As shown below, the IP Act maintains a clear distinction between communication 'content' and 'data' but this has been a source of criticism among experts. The importance of this distinction lies in its determination of applicable safeguards with stricter safeguard principles being applied to the interception of content.[678] The following sets out the definition of each before analysing the impact of this distinction on the protection of privacy in the digital age.

---

[676] IP Act, s 15(1)(b).
[677] Anderson report (n 158), Chapter 15, para 12.
[678] Chapter 2, section 2.1.4 set down the stricter and general safeguard principles developed by the ECtHR in its surveillance jurisprudence.

1.2.1 Communications data: 'entity' vs. 'events'

There are two types of communications data under the IP Act: 'entity' and 'events' data. 'Entity data' is information about an 'entity' (a person or thing)[679] and how it relates to a telecommunications system.[680] It is comparable to 'subscriber information' under RIPA which referred to customer information held by telecommunication operators.[681] However, 'entity data' is broader than 'subscriber information' because: (i) it does not only refer to customers and, (ii) the definition of 'telecommunication operators' has been expanded to include private companies like Facebook, Google, Apple, and Yahoo.[682] 'Entity data' can therefore include information like phone numbers, IP addresses, and home addresses.[683]

'Entity data' is distinguished from 'events data' which includes

> 'any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunications system where the event consists of one or more entities engaging in a specific activity at a specific time.'[684]

Therefore, 'events data' can include information on

> 'the fact someone has sent or received an email, phone call, text or social media message; the location of a person when they made a mobile phone call or the Wi-Fi hotspot that their phone connected to; or, the destination IP address that an individual has connected to online.'[685]

---

[679] IP Act, s 261(7).
[680] Ibid, s 261(3).
[681] RIPA, s 21(4)(c).
[682] IP Act, s 261(10).
[683] Home Office, *Explanatory notes to the Investigatory Powers Act 2016*, para 727.
[684] IP Act, s 261(4).
[685] Ibid.

‘Events data’ is considered more revealing than entity data and thus requires a higher level of authorisation for its acquisition.[686]

The above distinction between entity and events data has been criticised for being limited in use in the current technological landscape. Privacy International, for example, notes the different types of data arising from modern technology:

> ‘data about a phone call over a landline (eg two BT numbers shared a connection for 13 minutes) is vastly different than each ‘event’ within a chat session (eg two subscribers at locations X and Y interacted 97 times over a 13 minute period – sometimes with longer gaps and larger messages, other times with fast messaging indicating agreement or disagreement).’[687]

The London Internet Exchange (‘LINX’) also notes that the incorporation of private corporations into the definition of ‘telecommunications operators’ expands the type of information open to acquisition under ‘entity data:’

> ‘Amongst the types of companies that now fall within the new definition of a telecommunications operator [are] social networking sites and online messaging services. This means that Apple, Facebook, Google, Microsoft, Yahoo! and others will all be considered telecommunications operators within the meaning of the Draft Bill. And everything they know about anyone will be considered “entity data,” other than that which is events data.’[688]

---

[686] Ibid, schedule 4.
[687] Privacy International written evidence to the Joint Committee on the Draft IP Bill (IPB0120). See also, the Home Office written evidence to the Joint Committee on the Draft IP Bill (IPB0146) which lists examples of the different types of data and content for different forms of communication at paras 514-17. See also LINX written evidence (IPB0097). It is evident from these examples just how much more information is now available from digital communications than compared with postal communications.
[688] LINX ibid para 37.

LINX subsequently deems it 'remarkable' that the IP Act does not distinguish between different types of entity data given that some of this information can be equally, if not more, revealing than content.[689]

1.2.2 Communications content

The 'content' of a communication is defined in the IP Act as

> 'any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be expected to be the meaning (if any) of the communication.'[690]

However, 'content' disregards any meaning arising from the fact of a communication[691] or any data relating to the transmission of the communication.[692] The word 'meaning' in the above definition of content has come under fire for being a non-technical and subjective term. Dr Paul Bernal notes that it is possible to derive 'meaning' from almost any type of data.[693] Graham Smith also queries: 'for a computer to computer communication, what is the meaning of "meaning"?'[694]

Despite such criticism of this definition, it can still be considered an improvement on RIPA which failed to define 'content' in spite of its use throughout the Act.[695]

1.2.3 Content vs. data: in action

Having established the definitions of communications 'content' and 'data,' this section examines how this distinction is used in the IP Act, specifically in relation to the bulk

---

[689] Ibid para 39.
[690] IP Act, s 261(6).
[691] Ibid, s 261(6)(a).
[692] Ibid, s 261(6)(b).
[693] Paul Bernal written evidence to the Joint Committee on the Draft IP Bill (IPB0018), para 6.1.
[694] Graham Smith written evidence to the Joint Committee on the IP Bill (IPB0126), para 41. See also BT's supplementary written evidence to the Joint Committee on the Draft IP Bill (IPB0151) where it suggests the word 'substance' be used instead of 'meaning,' at para 208.
[695] See, for example, RIPA ss 3(1)(b), 3(5), 12(8), 106(8), 16(1), 33(2), 45(1).

powers. The impact of the content-data distinction on the IP Act's protection of privacy under Article 8 ECHR is then examined in Chapter 5.

Figure 1 (below) shows that the distinction between 'content' and 'data' determines who can apply for a bulk power warrant and in what circumstances. It demonstrates that greater restrictions and requirements are placed on the authorisation, use, and access to bulk interception and bulk Equipment Interference powers. The data-focussed powers on the other hand ('BCD' and 'BPD') can be accessed by more actors and used domestically.[696]

Bulk power	**Interception**	**BCD**	**EI**	**BPD**
SIAs only?	YES	YES	YES	NO
Foreign-focussed?	YES	NO	YES	NO
Content included?	YES	NO	YES	YES
National security purpose required?	YES	YES	YES	NO
Power used by?	GCHQ	MI5, GCHQ	GCHQ	ALL

Figure 1: Source: Report of the bulk powers review, at 2.3

Targeted power	**Interception**	**EI**
SIAs only?	NO	NO
Domestic-focussed?	YES	YES
Content included?	YES	YES
National security purpose required?	NO	NO
Power used by?	GCHQ, MI5, LEAs	GCHQ, MI5, LEAs

Figure 2

Evidently, the content-focussed powers are treated as more intrusive than the data-focussed powers in the Act. However, whilst the information *about* a communication may have typically been less revealing than its content in previous analogue eras, this is no longer the case in the digital age. Communication 'data' is highly amenable to aggregation and Big Data analysis techniques which can seriously interfere with both individual and societal privacy interests. The use of Big Data techniques for the

[696] For discussion of BCD and BPD powers see section 2 (below).

processing of data gathered under the bulk powers was confirmed in the 'Operational Case for Bulk Powers' which stated that the the techniques used were similar to those implemented by corporations to navigate substantial quantities of data and identify patterns of behaviour.[697] For example, Amazon uses a technique called 'collaborative filtering' to identify similar user preferences and to recommend products based on those similarities (eg 'Other people who bought this product also bought…').[698] There are many different types of techniques and some involve more human input than others. For instance, analysts might need to input keywords for a computer to subsequently apply to a database. Other techniques are more autonomous in the sense that machines identify patterns without the need for direct human instruction.

Different types of machine analysis will have different implications for privacy. For example, more autonomous techniques (those requiring less human input) are less transparent as the machine might reason through data in a way that is not obvious to a human. Consequently, human explanation and scrutiny of such independent machine analysis can be limited.[699] More direct techniques (those requiring greater human input) are more transparent but are also more prone to error with keyword searches generating more 'false positives,' or indeed, 'false negatives.'[700] For example, terrorists might adapt their language to avoid being caught in the government's surveillance net.

The effectiveness of these techniques also depends on the quality of the data. Where data is incomplete or inaccurate – which is not uncommon upon the removal of data from its original context – false inferences may be drawn about a person who might consequently suffer injustice, discrimination, or inappropriate decisions being made

---

[697] Home Office, *Operational case for bulk powers*, para 3.3 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf> accessed 24 June 2018.
[698] For further discussion on this see Pariser (n 538) 28-29.
[699] See Eyal Benvenisti, 'Upholding democracy amid the challenges of new technology: what role for the law of global governance?' (2018) 29 European Journal of International Law 9; Teresa Scassa, 'Law enforcement in the age of big data and surveillance intermediaries: Transparency challenges' (2017) 14 Scripted 2.
[700] For more information on the different types of issues facing autonomous and directed machine analysis and their human rights implications see, Peter Marguiles, 'Surveillance by algorithm: the NSA, computerised intelligence collection, and human rights' (2016) 68 Florida Law Review 1045.

about them. The Bichard Inquiry into the murder of Holly Wells and Jessica Chapman in 2003 demonstrates how human input error can result in persons 'slipping through the net.'[701] Eight separate sexual offences were alleged against murderer Ian Huntley, but due to a data input error he was able to be employed at the girls' school as a caretaker.[702]

Furthermore, due to the black-boxing of Big Data techniques (especially in the case of autonomous machine analysis) errors and injustices resulting from inaccurate data are incredibly difficult for individuals, regulators, and the courts to challenge and correct.[703] This was highlighted by medConfidential in its written evidence to the Joint Committee on the Draft IP Bill regarding the power to gather, analyse, and store 'bulk personal datasets' ('BPDs').[704] It noted:

> 'there is no clarity on the use of BPD by the security and intelligence agencies…only a description that they may be collected, and kept for as long as the agencies believe they may be useful.'[705]

Thus, aside from the fact that such datasets are gathered and stored, there is no information or detail as to how they are processed or used.

In addition, if algorithms are not designed with care they can be more discriminatory than humans by reflecting the 'social mores to the culture they're processing.'[706] Pariser provides the example of a software that helps companies search through resumes for talent: the algorithm might 'learn' that only white candidates are being picked from its results and so proceeds to exclude non-white candidates from its subsequent searches in order to be maximally efficient.[707] In a national security setting,

---

[701] The Bichard Inquiry, *The Bichard inquiry report* (2004, HC653).
[702] Ibid.
[703] This danger could be offset somewhat by strong notification requirements, however, as shown in Chapter 5, these do not exist within the IP Act. See Chapter 5, section 2.2.1.5.
[704] See Part 2, section 2.2.1 (below) for definition of BPDs.
[705] In fact, it was also argued by witnesses that even the types of data likely to be included within BPD is unclear as the aforementioned examples listed in the *Operational case for bulk powers* (n 697) are already available to SIAs.
[706] Pariser (n 538) 129.
[707] Ibid.

an algorithm used to search for potential suspects might 'learn' that only certain races or areas are being targeted for further inspection by analysts and so would adjust its search and results accordingly. Consequently, the use of algorithms could lead to an over-emphasis on certain races, religions, or geographical areas and an under-emphasis on those the algorithm has learned to be lower-risk.[708] Not only does this risk the discrimination and marginalisation of certain populations, but it also threatens to undermine national security efforts by excluding those who do not fit into the algorithm's 'learned' stereotype of a threat or suspect.

State use of such data-mining practices can also have a chilling effect on individuals' freedom of speech and association with people avoiding certain groups or restricting their expression of beliefs online for fear of falling within the search criteria of an algorithm.[709] As noted by Lyon, 'with Big Data there is no anonymity; all too often, interest slides seamlessly from causes to correlations.'[710] Indeed, the gravity of such dangers posed by Big Data processing techniques are reflected in the GDPR which grants data subjects the right to not be subject to a decision based solely on automated processing which will have legal or similarly significant effects.[711]

On the basis of the above, this thesis endorses Paul Bernal's conclusion that 'data' is not 'less' intrusive than 'content,' it is 'differently' intrusive' and, as such, concludes that the maintenance of this dubious distinction in the IP Act poses a dangerous risk to privacy.[712] However, as shown in the following chapter, the same content-data distinction also appears to permeate the ECtHR's application of Article 8 ECHR in surveillance cases with only general safeguards being applied to data-focussed powers.

---

[708] For discussion on risks and consequences of big data processes see: Ann Bevitt and Laura Dietschy, 'GDPR series: the risks with data profiling' (2016) 17 Privacy & Data Protection 6; David Lyon, 'Surveillance, Snowden, and big data: capacities, consequences, critique' (2014) Big Data & Society 1.

[709] This is supported by the 2015 report of the UN Special Rapporteur on Freedom of Expression where it was held that encryption is fundamental to freedom of expression as it protects against unjustified interferences. It follows that wide-reaching internet surveillance encroaches upon the individual's privacy online and so too, therefore, their freedom of expression, see David Kaye, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' A/HRC/29/32 (United Nations, 22 May 2015) at 7.

[710] Lyon, *The culture of surveillance* (n 1) 165.

[711] GDPR (n 645) Art 22.

[712] Paul Bernal (n 693) para 3.9.

Thus, it is perhaps not only the IP Act that needs to attune to the technocultural realities of the contemporary surveillance landscape in this respect. This is considered further in Chapter 5.

1.2.4 Summary

On the basis of the above, this section concludes that the IP Act's failure to acknowledge the collapse of the content-data distinction undermines its relevancy in the digital age as it insists upon a distinction that is no longer viable. This is to the detriment of privacy with weaker safeguards being applied to data-focussed powers (the legality of which is examined under Article 8 ECHR in the following chapter).

This conclusion contrasts with that of the Home Office which commends the Act's definitions of content and data for striking

> 'a balance between the operational requirements of the intelligence agencies to protect the public from terrorists and serious criminals, while protecting the most private information with stringent safeguards.'[713]

The Crown Prosecution Service has also praised the definitions for being 'both sufficiently clear and viable,' and making 'a helpful contribution to clarifying what is currently a complex area.'[714]

However, privacy scholars, NGOs, and network technology experts have been considerably less complementary of the definitions, condemning them for failing to recognise that technology has challenged the credibility of the traditional distinction between content and data. For example, Open Intelligence submitted to the Joint Committee on the IP Bill that

> 'on a technical level distinguishing between content and communications data as far as web use is concerned is questionable,

[713] Home Office written evidence (n 687) para 14.
[714] Crown Prosecution Service written evidence to the Joint Committee on the Draft IP Bill (IPB0081).

> not least because an Internet connection is most often being used for multiple services simultaneously, with data packets mixed together.'[715]

Liberty also notes that modern internet and smartphone usage has moved us beyond the simplicity of postal communications where, 'everything inside the envelope is content, everything on the outside communications data.'[716] Today, there is significantly more information that can be gathered from information *about* a communication than was previously the case in the analogue era. The value of non-content data was confirmed in the ISC's report where it noted that, 'the primary value of bulk interception to GCHQ was not in reading the actual content of communications, but in the information associated with those communications.'[717] As remarked by former director of the NSA and the CIA, General Michael Hayden, intelligence and security agencies 'kill people based on metadata.'[718]

The above distinction between content and data also provides insight into the IP Act's approach towards the public-private dichotomy in the digital age. As shown in Chapter 3, technology has prompted the migration of typically 'private' activities and interactions to more 'public' settings (from the home to online, for example), and vice versa.[719] Consequently, highly spatial concepts of the private and public spheres are becoming unbefitting legal 'boundary-markers' within the modern digital society.[720] However, when looking at the above distinction between 'content' and 'data' it is evident that the IP Act holds on to a more traditional, spatial notion of privacy for whilst it does offer some protection to communications data, it ultimately protects the

---

[715] Open Intelligence written evidence to the Joint Committee on the Draft IP Bill (IPB0066), para 36.
[716] Liberty written evidence to the Joint Committee on the Draft IP Bill (IPB0143), para 30.
[717] ISC report (n 634) para 80.
[718] At 'the John Hopkins foreign affairs symposium presents: the price of privacy: re-evaluating the NSA' (John Hopkins University, 1 April 2014) <https://www.youtube.com/watch?v=kV2HDM86XgI> accessed 30 October 2017. The Joint Committee on the Draft IP Bill also acknowledged that communications data now has the potential to be 'very intrusive,' in Joint Committee on the Draft IP Bill report (n 670) paras 357-362.
[719] This was demonstrated by analysis of 'sites of third wave surveillance' in Chapter 3, Part 2.
[720] As argued in: Galic et al (n 64); Nissenbaum (n 22); Joel Reidenberg, 'Privacy in public' (2014) 69 University of Miami Law Review 141; Lilian Edwards and Lachlan Urquhart, 'Privacy in public spaces: what expectations of privacy so we have in social media intelligence?' (2016) 24 International Journal of Law and Information Technology 279.

'inside' of a communication (the content) to a far greater extent than its 'outside' (the data). This is despite the 'outside' being capable of providing enough information for security agencies to carry out lethal force, as per General Hayden. The rationale behind weaker authorisation requirements for the acquisition and use of communications data is thus highly questionable. Although, as shown in the following chapter, it appears that the ECtHR functions on a similarly outdated distinction between content and data when determining Article 8 claims in surveillance cases.

In summary, it is evident that the drafters of the IP Act have tried to improve upon RIPA by formulating a definition for 'content' and replacing contentious terms like 'subscriber information' with 'entity' and 'events' data. It is also clear that a broad, technologically-neutral approach has continued to be used in order to prevent the law from becoming prematurely obsolete within the fast-moving context of the current technological landscape and to capture the multitudinous array of communication technologies that exist therein.[721] However, in its attempt to account for the numerous forms of communication that now exist in the digital age, the IP Act has failed to appreciate fundamental aspects of the very technology it seeks to take into account, such as, the significance of data produced by digital communications.

Therefore, whilst the IP Act faced the difficult task of developing definitions that possessed enough breadth to capture the different types of communication that now exist in the digital age, it has failed to recognise the blurring of content and data - reinforcing this distinction as opposed to recognising its disintegration. As shown in Chapter 5, this has resulted in weaker safeguards being applied to data-focussed powers than content-focussed powers. This poses serious risks to privacy in the contemporary surveillance landscape where state surveillance regimes are increasingly geared towards the gathering and processing of communications data rather than content. The distinction between content and data in the IP Act thus fails to reflect the

[721] Home Office written evidence (n 687). Technologically neutral language was also recommended in the Anderson report (n 158) in chapter 3 at para 4.1.

dangers to privacy posed by the increasing emphasis on communications data in the contemporary surveillance landscape.

1.3 'Bulk' vs. 'targeted'

Inherent to the bulk powers is their distinction from targeted powers, with the latter being treated as less invasive than their bulk equivalents. This is demonstrated in Figure 2 (above), which shows that targeted interception and EI powers can be applied for and used by more bodies (LEAs as well as SIAs) than bulk powers. Presumably, this is premised on the belief that targeted powers are directed at specified individuals as opposed to unspecified masses and, therefore, incur fewer invasions of privacy and require fewer controls and restrictions on their use. However, the problem with this assumption is that the 'targeted' warrants in the IP Act can be used thematically, meaning that groups of people, organisations, and locations can fall within their scope. For example, targeted interception is a domestic-focussed power that can be used against: (i) a group of persons who share a common purpose or who (may) carry on a particular activity, or; (ii) a group of persons, organisations, or premises for the purposes of a single investigation, or operation.[722] Furthermore, a targeted interception warrant need only name or describe as many of the persons, organisations, or premises as is reasonably practicable to do so.[723] Despite not being officially described as 'thematic,' warrants based on a theme as opposed to a specified individual, organisation, or premise might reasonably be referred to as such.

In comparison to bulk interception, the targeted version *is* narrower in scope for whilst not all subjects must be specified in a targeted warrant, at least some should be. Bulk interception warrants, on the other hand, do not require persons to be connected by a 'common purpose' or activity. However, as noted by the Centre for Technology and Democracy, the language of targeted interception and EI warrants

[722] IP Act, s 17(a)(b).
[723] Ibid, s 31(4)(b).

> ‘does not, by its terms, exclude the possibility that everyone who belongs to a certain trade union, political party or book club; visits a certain shop; attends (or has friends or family members who attend) a certain house of worship…uses a particular e-mail or instant messaging service may experience very serious privacy intrusions pursuant to a ‘targeted’ warrant in a manner that cannot reasonably be regarded as foreseeable.’[724]

Thus, the thematic nature of targeted interception powers

> ‘transforms what are presented as domestic “targeted” warrants into warrants that permit general surveillance in the hope of determining who, amongst potentially millions of people, might be engaged in the activity in question.’[725]

The Joint Committee on the Draft IP Bill also noted the breadth with which targeted interception and EI warrants might be used. It subsequently recommended that the Bill be amended so that these warrants cannot be used as a way to issue thematic warrants concerning a large number of people.[726] Although, evidently this recommendation was not incorporated into the final version of the Act.

Thematic interception powers were most recently challenged in the case of *Zakharov v Russia* where the ECtHR held that the authorisations for interception warrants

---

[724] Centre for Technology and Democracy written evidence to the Joint Committee on the Draft IP Bill (IPB0110).
[725] Matthew Ryder QC written evidence to the Joint Committee on the Draft IP Bill (IPB0142). Although Theresa May takes up against this, maintaining that ‘it will not be possible to use a thematic warrant against a very large group of people,’ see Therese May oral evidence to the Joint Committee on the Draft IP Bill, Q 276.
[726] Joint Committee on the Draft IP Bill (n 672) paras 461-468, recommendation 38. Also, David Anderson had recommended in AQT the continued use of thematic warrants but only in so far as they were to be used ‘against a defined group or network whose characteristics are such that the extent of the interference can reasonably be foreseen, and assessed as necessary or proportionate, in advance,’ see Anderson (n 158) para 14.61.

> ‘must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers, or other relevant information.’[727]

The thematic nature of ‘targeted’ warrants thus undermines the IP Act’s distinction between targeted and bulk powers as the former effectively enables ‘bulky’ (if not mass) surveillance of communications at home. Thus, the only real aspect distinguishing ‘targeted’ from ‘bulk’ powers appears to be where they are predominantly used (ie at home or abroad), as opposed to any substantive difference in scope. Perhaps, therefore, a more accurate distinction than ‘targeted’ and ‘bulk,’ would be ‘bulk’ and ‘bulkier’ surveillance.

1.4 Summary

It is unclear why the above distinctions have been maintained in the IP Act given the overwhelming evidence against their relevance in the digital age. Perhaps, they are used out of habit or to instil structure and boundaries in an increasingly unstructured and boundary-less technological world - an attempt to try and reinforce distinct spheres for the creation of clear and coherent laws. Alternatively, it could be argued that unworkable dichotomies have been purposefully maintained to facilitate a permissive regime of surveillance and maintain a clear pathway to gathering and accessing as much valuable data as possible.

Ultimately the reasons behind the use of these distinctions cannot be definitively answered within the remit of this thesis. However, it *can* be concluded that the IP Act struggles to deal with the collapse of dichotomies and, as a result, its powers are based on outdated distinctions that lack relevancy and meaning in the digital age. In turn, individuals are exposed to highly intrusive and bulk(y) state surveillance practices that (as shown in Chapter 5) fail to be accompanied by equally strong safeguards. Although, as also demonstrated in Chapter 5, the ECtHR appears to maintain a

---

[727] *Zakharov v Russia* (n 204) para 264. *Zakharov* is discussed at length in Chapter 5, section 2.2.

similarly problematic distinction between content and data when determining applicable safeguards. Thus, the extent to which the ECHR provides a safety net for practices slipping through the gaps of the IP Act is questionable.

2 Positioning participation

The sites of third wave surveillance examined in Chapter 3 (social media and smartphones) demonstrated the various ways in which individuals now actively participate in surveillance. This can be for a range of different purposes, including: entertainment; self-care; empowerment; self-actualisation; and, sociality. Alongside the benefits of a more democratised surveillance landscape, it was warned that an over-emphasis on the participatory turn in surveillance could lead to the under-regulation of surveillance practices and unjustified extension of the state's surveillance reach; with individuals' being viewed as putting everything 'out there' and subsequent surveillance of that information being exempt from, or at least subject to weaker forms of, legal protection.[728] It is thus important that the participation of the individual is properly positioned so that privacy is preserved in the digital age.

This section therefore establishes how the participation of the individual is positioned under the IP Act. This is achieved via an analysis of the Act's bulk data-focussed powers: 'Bulk Communications Data' ('BCD') and 'Bulk Personal Datasets' ('BPD'). The impact of the Act's approach to participation is then subsequently assessed in terms of its impact on privacy under Article 8 ECHR in Chapter 5. The IP Act's approach to this aspect of the contemporary surveillance landscape and its subsequent impact on the protection of privacy will therefore be demonstrated.

2.1 Defining 'bulk'

Whilst no definition of 'bulk' is provided by the IP Act, David Anderson states that the Act proceeds on a narrow understanding of 'bulk powers' as they only relate to the gathering of bulk data by the government itself.[729] A broad definition of bulk powers,

---

[728] Galic et al (n 64) 745; Cohen, 'The surveillance-innovation complex' (n 472), 270; Christian Fuchs, 'Surveillance and critical theory' (n 477), 7.
[729] David Anderson QC Independent Reviewer of Terrorism Legislation, *Report of the bulk powers review* (Cm 9326, 2016) paras 1.4-1.7

on the other hand, would focus on the *amount* of data collected rather than *who* collects it.[730] Consequently, the narrow definition of 'bulk' excludes powers requiring the acquisition and retention of bulk data by service providers as this is achieved by private actors.[731]

Despite the bulk powers being described by critics as 'mass' surveillance, this has been vehemently rejected by the government with PM Theresa May explicitly stating that the UK does not, has never, and will never carry out 'mass' surveillance.[732] However, in light of the breadth of the bulk powers illustrated below, this appears to be yet another dubious distinction maintained in the Act.

Under the narrow definition of 'bulk,' there are four powers listed under Parts 6 and 7 of the IP Act: (i) bulk interception:[733] (ii) bulk acquisition (otherwise referred to as 'BCD');[734] (iii) bulk equipment interference ('bulk EI');[735] and, (iv) bulk personal datasets ('BPD').[736] Whilst there is a wealth of information and critical analysis available on each, word limit restrictions permit only a discussion of certain aspects of the bulk powers that help to illustrate the IP Act's approach to the participation of the individual.

2.2 Participation under the IP Act

This section argues that the participatory characteristic of the third wave fails to be appropriately positioned under the IP Act which consequently impacts its protection of privacy in the digital age. This is demonstrated via an examination of the data-focussed bulk powers listed under Part 6 of the IP Act: BCD and BPD. The suitability of the IP Act's approach to participation is assessed in terms of Article 8 ECHR in Chapter 5.

---

[730] Ibid para 1.6
[731] Ibid. For example, the power to require service providers to retain customers' 'Internet Connection Records' ('ICR') (essentially web logs) for a period of up to 12 months is not listed as a bulk power, but rather under Part 3: 'Targeted authorisations for obtaining data' (IP Act, s 62).
[732] Theresa May oral evidence (n 725), Q271.
[733] IP Act, part 6 chapter 1.
[734] Ibid, part 6 chapter 2.
[735] Ibid, part 6 chapter 3. For definition of EI see text to n 708.
[736] Ibid, part 7.

2.2.1 Definition of BCD and BPD

The IP Act provides for the acquisition of BCD[737] and BPD.[738] A BCD warrant requires the acquisition of domestic communications data by telecommunications operators, some of which might have to be specifically obtained if not already in its possession.[739] Data acquired under a BCD warrant is then aggregated into a single database as opposed to being held on multiple different databases by communication service providers as prescribed under previous data retention laws.[740]

BPD warrants require the collection of 'sets of information that includes the personal data relating to a number of individuals.'[741] 'The Operational Case for Bulk Powers' gave the following examples of a BPD database: a list of people holding passports; the electoral register; commercial data (such as the telephone directory); financial data; and, the firearm register.[742] As noted by the Investigatory Powers Commissioner, these examples are fairly unhelpful given that such datasets are already available to the security and intelligence agencies under existing legislation.[743] However, in a draft report summarising the findings of a 2017 audit of the operation of BPDs by the Investigatory Powers Commissioner's Office ('IPCO'), explicit reference was made to 'social media data' when discussing how agencies handle different BPD databases.[744] This indicates that content from social networking platforms can also be included in BPDs. Ultimately, however, the scope of BPD remains unclear.

---

[737] IP Act 2016, part 6 chapter 3. BCD were previously carried out under the Telecommunications Act 1984, s 94.
[738] Ibid, part 7. The government maintains that BPD powers are not new and that they were previously carried out under the Security Services Act 1989 (s 2(2)(a)) and the Intelligence Services Act 1994 (ss 2(2)(a) and 4(2)(a)). However, this is widely disputed by critics who argue that BPD powers are essentially new. For example, Eric King, argues that, 'simply because the agencies have interpreted law in a manner that they feel has made them lawful does not make them lawful' (see, Eric King, Oral evidence to the Joint Committee on the Draft Investigatory Powers Bill, Q202).
[739] IP Act, s 170.
[740] Data Retention Directive (n 641) and DRIPA 2014.
[741] IP Act, s 199(1)(a)(b). Nb s 199(1)(d) holds that 'personal data' has the same meaning as in the Data Protection Act 1998 except it can also include information relating to a deceased person.
[742] These were the examples listed in Home Office, *Operational case for bulk powers* (n 697) para 10.7.
[743] Christopher Graham Information Commissioner oral evidence to the Joint Committee on the Draft IP Bill (Q231).
[744] IPCO, 'Draft report summarising the findings of the 2017 BPD audit' (IPCO, 15 September 2017). Available via <https://privacyinternational.org/sites/default/files/2018-

Both BCD and BPD are predominantly used as investigative tools for national security or for detecting serious crime by: focusing intelligence efforts on suspected individuals; establishing links between suspects; verifying intelligence gained from other sources;[745] or, for identifying anomalies to expose hostile activity.[746] Both warrants must be applied for by the head of an intelligence service to the Secretary of State who can only issue a warrant following judicial authorisation, except for in 'urgent cases.'[747] All data acquired under BCD warrants and specific types of BPD containing 'protected data' can only be examined by an analyst for an approved 'operational purpose.'[748] Prior to human examination, data can be electronically searched and processed using Big Data analysis techniques. However, as discussed above, machine analysis can pose serious privacy issues regardless of whether a human is involved or not.[749]

2.2.2 Haystacks and needles

There is no limit to the quantity of data that can be requested under BCD or BPD warrants and the government maintains that the majority of data will not be of intelligence interest to SIAs.[750] Despite this, these powers are defended as being instrumental to national security and the detection of serious crime in the digital age 'where the benefits enjoyed by us all [online] are being exploited by serious and organised criminals, online fraudsters and terrorists.'[751] The bulk acquisition of

02/4.%20Open%20version%20of%20IPCO%20draft%20audit%20report%2015%20Sept.pdf> accessed 16 August 2018.

[745] Ibid, para 10.4.

[746] Anderson (n 158) para 8.19.

[747] IP Act, ss 166, 204, 205. Secretary of State's power to approve warrants in 'urgent cases' without judicial authorisation is listed under ss166 and 209 for BCD and BPD powers, respectively. This exception is discussed in more detail in Chapter 5, section 2.2.1.3.

[748] Examination of BCD and 'specific' BPD (ie those containing 'protected data') required under ss 161(3) and 205(4)(b) respectively. 'Operational purposes' are not listed in the IP Act, rather a list is maintained by the heads of SIAs which must be approved by the Secretary of State and is reviewed by the ISC and PM every 3 months and annually, respectively (IP Act, s 161(6)(10)).

[749] See section 1.3.1 'Content vs. data: in action' (above).

[750] Operational case for bulk powers (n 697), para 5.8.

[751] HC deb 4 November 2015, col 969. The utility of the bulk powers was also accepted in the Anderson, ISC, and RUSI reports.

communications data and personal datasets has subsequently been defended on the basis that it enables SIAs to

> 'sift through "haystack" sources without looking at the vast majority of material that has been collected – in order to identify and combine the 'needles,' which allow them to build an intelligence picture.' [752]

However, the assumption that vast 'haystacks' are required to find the 'needle' is challenged by evidence submitted to the Joint Committee on the Draft IP Bill with a number of experts underlining the danger of the 'haystack-needle' approach to national security efforts. For example, William Binney, former technical director of the NSA, argued that

> 'it is not helpful to make the haystack orders of magnitude bigger, because it creates orders of magnitude of difficulty in finding the needle…Using a targeted approach would give you the needles, and anything closely associated with them, right from the start.'[753]

It has also been argued from a mathematical perspective that the effectiveness of the haystack/needle approach is hindered by the number of 'false positives' thrown up by the haystacks:

> '[b]ecause of the base rate fallacy and the fact that terrorists are relatively few in number compared to the population as a whole, mass data collection, retention and mining systems…always lead to the swamping of investigators with false positives, when dealing with a large population.'[754]

Despite these concerns, BCD and BPD powers show that a haystack-needle approach has nevertheless been adopted by the IP Act with masses of 'hay' being gathered and retained in order to locate and investigate potential 'needles.' The disputed

---

[752] ISC report (n 634) (quoting written evidence submitted by the government) at para 51.
[753] William Binney oral evidence to the Joint Committee on the Draft IP Bill (Q239).
[754] Ray Corrigan written evidence to the Joint Committee on the Draft IP Bill (IPB0053).

effectiveness of this approach leads to questions of proportionality under Article 8 ECHR which are considered in Chapter 5.

Both BCD and BPD powers have been facilitated by changes in the digital age. They are possible because of changes in how we live our lives. As shown in Chapter 3, Web 2.0 has encouraged the transferral of (social) life online, resulting in the publicisation of what had traditionally been considered private.[755] Technological advances, such as the Big Data analysis techniques described in section 1.2.3 above, have also enabled individuals' data exhaust to be processed at great speed. However, as concluded in Chapter 3, just because the individual conducts more of her life online - thereby rendering it more visible, recordable, and, ultimately, surveillable - expectations of privacy over these now digitalised aspects of life are not necessarily negated.[756]

Despite evidence evidence that SOCMINT is gathered under BPD, it appears that BPD relates less to data exhaust than BCD based on the examples provided in the 'Operational Case for Bulk Powers' (eg electoral and firearm register, financial dealings, and travel data). These types of information have been recorded and searched by government agencies for many years. The difference, however, is that this information can now be accessed without individualised suspicion to carry out general searches. This is achievable due to technological developments as opposed to changes in how we live our lives. It is thus necessary to ask why, and indeed if, the addition of these datasets to the haystack is acceptable. This is considered in Chapter 5 via an analysis of BPD under Article 8 ECHR.

2.3 Summary

The above analysis of BCD and BPD has served to illustrate the IP Act's response to the role of the individual in the contemporary, third wave surveillance landscape. This response was characterised in terms of haystacks and needles, with vast haystacks of data being collected 'in case of' a needle hiding within. This approach has been facilitated by changes in the way we now live our lives (ie from the analogue to the

[755] See further Chapter 3, Part 2.
[756] See Conclusion of Chapter 3.

digital) that have contributed to our data exhaust, and technological advances in processing that make it possible to sift through vast volumes of data at higher speeds and lower costs. However, as argued in Chapter 3, just because the individual conducts more of her life online – thereby rendering it more visible, recordable, and ultimately surveillable – expectations of privacy over these now digitalised aspects of one's life are not necessarily negated. The failure to recognise such technocultural change risks laws being predicated on incorrect assumptions about individuals' expectations of privacy in the digital age which, in turn, can result in the unjustified extension of surveillance powers that lack necessary safeguards against abuse. This is demonstrated via an analysis of BCD and BPD powers under Article 8 ECHR in Chapter 5.

3 Group privacy

Building on the previous discussion of the 'haystack-needle' approach taken by the IP Act, this section underlines the need to develop a group privacy right in the contemporary surveillance landscape.

It was established in Chapter 2 that there currently exists very limited scope for group privacy claims to be made under Article 8 ECHR.[757] Whilst the 'mere existence' test developed in *Klass v Germany* established that victimhood can arise without actual and concrete harm being substantiated by the applicant, it was questioned whether this constituted a *real* group privacy right as it did not allow for groups to develop their identity and promote their interests (as a group) under Article 8. The following demonstrates the impact of this individualistic focus by establishing the difficulties in making an Article 8 claim based on the type of harm caused by BCD and BPD powers discussed above.

First, given that BCD and BPD powers gather, retain, and process the communications data and datasets of *everyone* as opposed to a specific person or specific group of persons, it is difficult for the individual to point to a specific and direct harm materialising from the use of these powers. Second, as shown in Chapter 3, individuals

[757] Chapter 2, section 4.

now lead an increasingly digitalised life which means they are contained in numerous different data flows and streams in the digital age. This makes it incredibly difficult for individuals to know when their data is being collected, by whom, and for what purpose. Without strong notification requirements (which as argued in Chapter 5, is the case with the IP Act), the individual is practically prohibited from invoking her Article 8 right as legal persons cannot, in principle, submit a claim under Article 8 on behalf of others. Third, the Big Data processes used to analyse information gathered under BCD and BPD powers, make it difficult to point to a clear and concrete interference with private life. This was noted by van der Sloot who explains that:

> 'New data-driven technologies generate large amounts of data from all aspects of society. Statistical correlations are detected by using smart algorithms. Group profiles are distilled and translated into policy decisions. With these types of Big Data processes, the individual interest is increasingly difficult to substantiate.'[758]

Thus, the wider the surveillance net gets, the more difficult it becomes for the individual to identify and substantiate the personal harm directly caused to them. As a result, it becomes difficult to challenge mass, data-focussed state surveillance regimes. However, as demonstrated in section 1.3.1 (above) harm *is* caused to the individual by powers like BCD and BPD - albeit a more indirect, less concrete harm than that caused by the wiretapping of a telephone or invasion of one's home. Rather, these mass, data-driven surveillance practices create a 'power relationship' by providing a birds-eye-view to the state over its citizens and society generally which enables behaviours to be learned and influenced accordingly.[759] Without strong safeguards and independent oversight, this power risks being used by states arbitrarily. Sloot notes that the mere existence of this power and capacity to use it arbitrarily can have profound effects on the individual who, 'can feel themselves curtailed in their freedom and will limit their

[758] Bart van der Sloot, 'A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principles' (2018) 34 Computer Law & Security Review 539, 542. Van der Sloot gives gives the example of the NSA gathering data on millions of people and asks what harm the average person suffered from those activities?
[759] Ibid 543.

behaviour in anticipation for fear of potential unknown consequences.'[760] Thus, as in the Panopticon, power becomes 'visible but unverifiable.'[761]

In light of the above, this thesis argues that greater scope for group privacy needs to be developed under Article 8 ECHR in order for the power relationship emerging from mass, data-focussed surveillance to be adequately checked and challenged. Consideration as to how this might be achieved is included in Chapter 6.

Conclusion

This chapter has explored the UK's approach to the contemporary surveillance landscape via an examination of the IP Act's response to the legal implications of the third wave identified in Chapter 3. The conclusions of this analysis are as follows.

First, distinctions maintained in the IP Act were examined to determine the extent to which the Act recognised the collapse of dichotomies in the digital age. It was shown that the IP Act has failed to adapt its boundary-marking concepts to reflect the convergence of previously distinct concepts in the digital age. This has left privacy in a highly precarious position. For example, the content-data distinction maintained in the Act means that weaker safeguards are applied to data-focussed powers on the (mistaken) assumption that data is less revealing than content. However, as argued above and in the following chapter, this is not always the case and stricter safeguards *should* apply to bulk data-focussed powers. Although, as shown in the following chapter, the ECtHR adopts a similar approach to content and data meaning that Article 8 ECHR does not necessarily form a safety net here.

Second, the IP Act's response to the participation of the individual was established. This was demonstrated via the BCD and BPD powers and characterised in terms of 'haystacks' and 'needles.' It was concluded that whilst the individual's participation in digital data exchanges has facilitated an extension of the state's gaze by rendering previously unseen aspects of life more transparent, the participatory characteristic of

[760] Ibid.
[761] See Chapter 3, Part 1, section 1.1 on Bentham's prison-panopticon.

the third wave landscape does not justify the extent to which the state's surveillance reach has been extended by the IP Act. Whilst increased policing online is clearly necessary given that the bad as well as the good now dwell here, the extent to which privacy and online security has been sacrificed 'in case of' there being a needle hidden among innocent communications and transactions raises serious issues of proportionality. This is investigated in Chapter 5 where it is considered whether the ECtHR's approach to proportionality would likely lead to the bulk powers being deemed unlawful under Article 8(2) ECHR.

Third, the IP Act's haystack-needle approach was used to underline the need for a strengthened group privacy right in the digital age. Whilst the highly individualistic nature of Article 8 ECHR was sufficient in previous eras, the emergence of bulk, data-focussed surveillance powers make it incredibly difficult for individuals to point to a concrete and specific harm. Consequently, scope to challenge this type of surveillance is significantly reduced and the state is left with a dangerously broad area of discretion. Accordingly, this section concluded that greater scope for group privacy needs to be developed under Article 8 ECHR in order for the power relationship emerging from mass, data-focussed surveillance to be adequately checked and challenged. Chapter 6 considers how this might be achieved.

Based on the above, this chapter concludes that the IP Act fails to attune to the technological and cultural changes that the contemporary surveillance landscape has undergone. The impact of this failure is explored in the following chapter in terms of its protection of privacy under Article 8 ECHR. Although, as will be shown, it appears that the ECtHR also struggles to adapt to the technocultural reality of the contemporary surveillance landscape.

Chapter 5 The UK approach under the ECHR

Introduction

This chapter critically assesses the impact of the IP Act's approach to the contemporary surveillance landscape in terms of its protection of privacy under Article 8 ECHR. The following aspects of the Act established in Chapter 4 are examined: (i) the haystack-needle response to the participation of the individual; (ii) the maintenance of outdated distinctions for the digital age. Chapter 4 also used the IP Act to underline the need for a group privacy right in the contemporary surveillance landscape. However, as the scope for such a right under Article 8 ECHR has already been established in Chapter 2, this need not be repeated here. Recommendations as to how group privacy might be strengthened under Article 8 ECHR are thus considered in the following chapter.

First, the impact of the haystack-needle approach on the protection of privacy will be examined. In Chapter 4, it was shown that individuals' participation in digital data exchanges has facilitated an extension of the state's surveillance powers under the IP Act. However, it was argued that this extension is not necessarily justified by such participation which, as shown in Chapter 3, is undertaken for the purposes of sociality, self-actualisation, and even empowerment. By framing this participation as an expression of the individual's ownership of surveillance, it is argued that expectations of privacy persist within realms of exposure (eg on social networking sites).[762] Therefore, this chapter examines the extent to which the IP Act's failure to properly position the participation of the individual has resulted in the unjustified extension of state surveillance powers that lack adequate safeguards against abuse. This is achieved via an examination of the BCD and BPD powers under Article 8 ECHR.

Second, the impact of the IP Act's failure to recognise the collapse of dichotomies on the protection of privacy is examined. In Chapter 4 it was argued that the distinction

[762] As concluded in Chapter 3, Part 2, section 1.4.

between ‘content’ and ‘data’ was outdated in the digital age and risked an inadequate system of safeguards being applied to data-focussed powers. This is explored here via an analysis of the different safeguards applied to content-focussed (interception and EI) and data-focussed powers (data acquisition, retention, and BPD) under Article 8 ECHR.

Whilst the main focus of this chapter is on the IP Act, consideration is also given to the suitability of the ECtHR’s application of Article 8 in the contemporary surveillance landscape. Potential weaknesses in its protection of privacy will be identified on the basis of discussion in previous chapters and supported by reference to the CJEU’s approach in its recent surveillance case law where it offers potentially stronger protection of privacy.

1 The haystack-needle approach under Article 8 ECHR

This section examines the legality and necessity of the BCD and BPD powers under Article 8 as means of determining the impact of the haystack-needle approach on the protection of privacy. Whilst the ECHR provides the benchmark against which the IP Act is assessed in this chapter, the suitability of the ECtHR’s approach is also evaluated in terms of the extent to which it provides a safety net for the protection of privacy in the digital age. This is achieved via a comparison with the CJEU’s approach to modern surveillance practices and its protection of privacy in its recent surveillance case law.[763] This section is structured as follows: (i) triggering Article 8(1); (ii) legality; (iii) necessity and proportionality; and, (iv) The CJEU’s approach: a way forward?

1.1 Triggering Article 8(1)

It was established in Chapter 2 that whilst expectations of privacy are limited over public information, the subsequent processing of that information can work to trigger Article 8(1).[764] The systematic collection and retention of public information by the state can also engage Article 8(1) due to the potential for processing that arises upon

[763] Namely in *DRI* (n 15) and *Tele2/Watson* (n 15).
[764] *Friedl v Austria* (n 185). See also *Peck v UK* (n 23) and discussion in Chapter 2, section 1.2.3.

its retention.[765] It follows that the systematic gathering and retention of data under BPD and BCD warrants would successfully engage Article 8(1) due to the significant potential for processing that subsequently arises.[766] It is thus necessary to assess the legality and necessity of these powers under Article 8(2).

1.2 Legality

In terms of legality, the BCD and BPD powers must have: (i) a basis in domestic law, and (ii) be accessible and foreseeable.[767] Evidently the powers have a basis in domestic law as they are prescribed by the IP Act. Attention thus turns to the accessibility and foreseeability of these powers.

The foreseeability requirement does not require that an individual be able to foresee when the authorities are likely to intercept his communications so that he can adapt his behaviour accordingly.[768] Although, the law does need 'to define the scope and conditions of exercise of the authorities' discretionary power.'[769] The legality requirement also demands the inclusion of sufficient safeguards and oversight, with stricter safeguard principles being applied to interception cases.[770] Otherwise, the more general safeguard principles will apply meaning that the relevant law need only define,

> 'the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.'[771]

Prior to the passing of the IP Act, the IPT held in *Privacy International v GCHQ* that the BCD and BPD powers were unlawful under Article 8(2) for a period of 17 years

---

[765] See *Rotaru v Romania* (n 229) and discussion in Chapter 2, section 1.3.2.
[766] Especially in light of Big Data techniques being used to process these vast datasets, see Chapter 4, Part 2, section 1.2.3.
[767] See Chapter 2, sections 2.1.1 and 2.1.2.
[768] *Malone v UK* (n 195), para 79. See Chapter 2, section 2.1.2.
[769] *Amann v Switzerland* (n 229), para 58. See Chapter 2, section 2.1.2.1.
[770] Stricter safeguards set out in *Kruslin v France* and *Huvig v France* (n 262), and *Valenzuala Contreras v Spain* (n 273). See Chapter 2, section 2.1.4.
[771] *Uzun v Germany* (n 280), para 62. See Chapter 2, section 2.1.4.2.

until being publically avowed in November 2015 and March 2015, respectively.[772] However, following the passing of the IP Act, this is no longer an issue as each now have a basis in domestic law and are thus accessible to the public. Thus, accessibility of these powers is unlikely to be an issue under Article 8(2).

With regard to the foreseeability of the BCD and BPD powers, it is unlikely that illegality will be found. This conclusion is based on the examination of the IP Act's safeguards and oversight in section 2 (below) where it is argued that the safeguards applied to BCD and BPD powers would likely fulfil the more general safeguard principles applied to these data-focussed powers by the ECtHR. It is thus necessary to assess the lawfulness of the UK's haystack-needle approach in terms of the necessity and proportionality requirements under Article 8(2).

1.3 Necessity and proportionality

As shown in Chapter 2, the ECtHR has typically adopted a procedural approach to the question of proportionality in surveillance cases by focussing on the existence of adequate and effective safeguards.[773] This enables the Court to avoid an in-depth analysis of the *proportionality strictu sensu* (balancing) branch of the test.[774] However, given that an in-depth examination of safeguards is carried out in section 2 below, this section will carry out a more substantive analysis of the proportionality test as seen in *S and Marper v UK*.[775] This enables a fuller critical assessment of the legitimacy, necessity, suitability, and proportionality of the BCD and BPD powers.[776]

First, it is unlikely that the powers would be considered contentious in terms of their legitimacy given that they serve national security and prevention of crime purposes, for which there exists a broad margin of appreciation.[777] Similarly, regarding the necessity of the regime, it would likely be accepted that there are advantages to having

---

[772] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, GCHQ, Security Service, and SIS* [2016] IPT/15/110 CH.
[773] See Chapter 2, section 3.2.1.
[774] Reasons for more procedural proportionality assessment given in Chapter 2, section 3.2.1.
[775] See Chapter 2, section 3.2.1.1.
[776] *S and Marper v UK* (n 235).
[777] See further Chapter 2, section 3.3.

comprehensive databases of communications data and personal datasets as they contribute to the purposes of the regime. However, on the basis of *S and Marper v UK* issues could potentially arise in relation to the suitability and balancing aspects of the test.

In *S and Marper*, the ECtHR questioned the suitability of the data retention scheme on the basis that the UK (excluding Scotland) was the only Council of Europe state to permanently store this type of data.[778] This led the ECtHR to question whether there existed 'relevant and sufficient reasons' behind the interference and to conclude that the same goal could have been achieved via less restrictive means.[779] However, the IP Act applies to the UK as a whole with only *mutatis mutandis* variations that take into account differences in institutional and jurisdictional dimensions.[780] Consequently, haystacks are created across the UK and so there is no great angle to be gained from considering other jurisdictions in the UK as there was in *S and Marper*. However, such an angle *could* be gained by looking to the CJEU's approach in *Tele2/Watson*.[781] It was held here that mass data retention powers under the Data Retention Directive constituted a disproportionate interference with privacy on the basis that the same goals could be achieved via more targeted powers.[782] Perhaps, therefore, this could prompt the ECtHR to apply more intensive scrutiny as it did in *S and Marper*. This is explored further in section 1.4, below.

Finally, in determining whether the powers achieve 'a fair balance between competing public and private interests,' the ECtHR in *S and Marper* examined the consequences of the blanket and indiscriminate retention of the concerned material. In reaching the conclusion that a fair balance had not been struck under the data retention scheme, the ECtHR underlined: the impact on the private life of individuals (especially minors); the risk of increased stigmatisation; and, the negative impact on societal interests (like

---

[778] See Chapter 2, section 3.2.1.1.
[779] *S and Marper v UK* (n 235) paras 114-116.
[780] See for example, IP Act, s 21 which makes provision for Scottish Ministers to issue interception warrants.
[781] *Tele2/Watson* (n 15).
[782] *Tele2/Watson* (n 15). This was recently upheld in the domestic case of *R (The National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department & Anor* [2018] EWHC 975 (Admin).

the presumption of innocence).[783] These consequences are all relevant to BCD and BPD powers which can disclose highly sensitive details about a person's life and, as highlighted in Chapter 4's critical analysis of the content-data distinction, also carry serious risks of stigmatisation and discrimination.[784]

It therefore appears that the BCD and BPD powers *could* be successfully challenged on the basis of proportionality. However, it is uncertain whether such a full analysis of proportionality would be carried out by the ECtHR in light of its preference for a more pragmatic proportionality assessment. A wide margin of appreciation is applied in surveillance cases where states seek to justify interferences on national security grounds and so the Court might elect to focus on the sufficiency of safeguards in the IP Act as opposed to conducting a more substantive analysis of the proportionality of BCD and BPD powers.[785]

However, recent ECtHR case-law could indicate an evolution in the ECtHR's approach. Notably, in *Szabo and Vissy v Hungary* regarding the mass surveillance of communications, the ECtHR held that

> '[g]iven the technological advances since the *Klass and others* case, the potential interferences with email, mobile phone, and Internet services as well as those of mass surveillance attract the Convention of private life *even more acutely*.'[786] [emphasis added]

This demonstrates an awareness on behalf of the ECtHR of the key role of digital communications in modern society and the subsequently heightened risk to privacy posed by their mass surveillance. Therefore, this could lead to a more intensive scrutiny being applied by the ECtHR in modern surveillance cases. Should this be the case, the ECHR would provide a stronger safety net for the protection of privacy against mass, data-focussed powers like BCD and BPD. This would, in turn, work to correct the positioning of participation under the IP Act. However, it is too early to

---

[783] *S and Marper* (n 235), paras 122-125. See Chapter 2, section 3.2.1.1.
[784] See Chapter 4, Part 2, section 1.2.3.
[785] *Klass v Germany* (n 199), para 49. See further Chapter 2, section 3.3.
[786] *Szabo and Vissy v Hungary* (n 266), para 53.

provide a definitive conclusion on this presently. Therefore, should such a development *not* occur, and a wide margin of appreciation continue to be applied by the ECtHR, it is predicted that a justifiable interference with Article 8 would be found regarding BCD and BPD powers due to the (quasi-) participation of the individual in digital data exchanges. On this basis, it is argued that the ECHR fails to correct the positioning of participation under the IP Act, leaving the individual (and society as a whole) vulnerable to mass state surveillance practices. Accordingly, it may be concluded that the ECHR, as well as UK surveillance law, needs to attune to the technocultural realities of the contemporary surveillance landscape in order to preserve privacy in the digital age.

Having established potential weaknesses in the ECtHR's approach to determining discretion and proportionality in surveillance cases, the following considers whether the judgment of the CJEU in *Tele2/Watson* might offer something of a safety net for the protection of privacy against BCD and BPD powers. This builds on the previous discussion in Chapter 2 on the differences between the ECtHR and CJEU's approach to determining discretion.[787]

1.4 The CJEU's approach: a way forward?

In the *DRI* case, the CJEU held that the obligation to retain communications data under the Data Retention Directive constituted a disproportionate interference under Articles 7 and 8 of the EU's Charter of Fundamental Rights – the rights to privacy and the protection of personal data, respectively. [788] However, the CJEU noted that the retention of metadata *could* be compatible with Articles 7 and 8 where it fulfils an operational purpose such as (but not limited to) fighting serious crime or terrorism, but that it must be strictly necessary to pursue this objective.[789] Furthermore, in order to be compliant with Articles 7 and 8, access to retained metadata had to be limited to

[787] See Chapter 2, section 3.3.1.
[788] *DRI* (n 15), paras 39-40.
[789] Ibid, paras 38-42.

the investigation of serious crime and be subject to prior independent review (not necessarily by a court).[790]

On the basis of *DRI,* the applicants in *Tele2/Watson* challenged the compatibility of the bulk data retention scheme under DRIPA 2014 with the 'ePrivacy Directive.'[791] In reaching the conclusion that the bulk data retention powers were unlawful, the CJEU went further than in *DRI* by holding that bulk data retention must: (i) be limited to purposes of national security, defence, public security, and serious crime;[792] (ii) be the exception and not the norm;[793] and, (iii) be 'genuinely and strictly' necessary for the purpose sought.[794] Regarding access to retained bulk data, it held that under the 'ePrivacy Directive' data can only be accessed where it strictly corresponds to the same purpose for which it was retained and must be limited to what is strictly necessary.[795] Again, the CJEU underlined the importance of prior independent authorisation and added that notification to persons whose data had been accessed should be carried out as soon as is practicable.[796]

Although DRIPA has now been replaced by the IP Act, it was recently held in *R (on the application of National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department* that the power of the Secretary of State to require telecommunications operators to retain specified communications data for up to 12 months under s 87(1) of the IP Act was incompatible with EU law in so far as it: (i) allows the retention of data for purposes not related to 'serious crime,' (thus going beyond the purposes listed in *Tele2/Watson*); and, (ii) provides access to retained data that is not subject to prior review by a court or independent body.[797]

---

[790] Ibid, para 62.
[791] *Tele2/Watson* (n 15); Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37 (ePrivacy Directive); Articles 7 and 8, and s 52(1) of the Charter. *Tele2/Watson* subsequently upheld in *Secretary of State for the Home Department v Watson MP & Ors* [2018] EWCA Civ 70.
[792] *Tele2/Watson* (n 15) para 90.
[793] Ibid, paras 104-107.
[794] Ibid, para 109.
[795] Ibid, para 115.
[796] Ibid, paras 120-121.
[797] *Liberty v SS for the Home Department* (n 782).

Other aspects of the claimant's argument were not successful, including the claim that Part 4 of the IP Act allowed for 'general and indiscriminate' retention of communications data. The Divisional Court rejected this on the basis that the power can only be used where it is deemed 'necessary and proportionate' by the Secretary of State and a Judicial Commissioner.[798] However, this conclusion appears to function on a fairly narrow interpretation of the CJEU's ruling in *Tele2/Watson* by maintaining that the list of safeguards prescribed by the CJEU[799] were merely examples as to how Member States *might* restrict retention schemes as opposed to constituting a prescriptive list of safeguards to be enshrined in legislation.[800] However, on the basis of the clear and explicit language used by the CJEU in *Tele2/Watson*, it is held here that it *did* intend for restrictions (such as the setting of a geographical location and time period) to be included in domestic laws. Consequently, the Divisional Court erred in its interpretation of the CJEU's judgment on this point.

Although *Tele2/Watson* only deals with the retention of communications data and not its acquisition and use, a preliminary reference has been submitted to the CJEU to determine the applicability of the *Tele2/Watson* principles to BCD powers following a case brought by Privacy International in 2017.[801] Privacy International argued that BCD powers were within the scope of EU law, meaning that the principles were applicable and that the IP Act fails to comply with EU law.[802] However, the government claimed that the national security purpose of BCD renders it outwith the scope of EU law on the basis of Articles 4 and 5 of the Treaty of the European Union.[803] The IPT demonstrated support for the government's position, emphasising

---

[798] Ibid, paras 128, 133, and 135. Judicial commissioners are part of the new oversight regime under the IP Act. Their role is discussed below in section 2.1 and 2.2.1.3.
[799] *Tele2/Watson* (n 15), paras 106, 108-111.
[800] *Liberty v SS for the Home Department* (n 782), para 124.
[801] *Privacy International v GCHQ* (n 772). Nb the BPD powers were included in Privacy International's challenge but have been excluded from the reference to the CJEU on the basis that compulsory powers are not used to obtain BPDs. Accordingly, the reference only concerns the applicability of EU law to the BCD regime. Furthermore, whilst the case concerned the use of BCD under s 94 of the Telecommunications Act 1984, the powers remain largely unchanged under the IP Act and so a reference from the CJEU will retain relevance to the current BCD regime.
[802] Ibid, para 20.
[803] Ibid, para 32. Art 4 TEU states essential functions of Member States (including national security) are not conferred to the Union. Art 5 states that the the limits of the Union competences are governed by the principle of conferral.

the national security purpose of the BCD regime and its difference from the problematic retention of communications data under DRIPA at issue in *Tele2/Watson*.[804] However, the IPT has referred the issue to the CJEU for clarification on the impact and meaning of the *Tele2/Watson* judgment.[805]

The CJEU is yet to rule on the case so only a prediction can be made here. Whilst there are aspects of the IPT's judgment that are fundamentally flawed from a privacy perspective (especially its proportionality assessment of the BCD regime),[806] with regard to the applicability of the *Tele2/Watson* principles it seems unlikely that the CJEU would consider BCD within the scope of EU law given the clear national security purpose of this power. This is supported by *The European Parliament v Council of the EU* regarding the sharing of airline passenger data ('PNR data') with US authorities.[807] It was held here that the national security purposes of the regime rendered it outwith the scope of Community Law.[808] On this basis, it is likely that the *Tele2/Watson* principles will remain restricted to the retention of data under the IP Act which is aimed at criminal investigations and will not, therefore, be extended to safeguard privacy from the bulk acquisition and use of BCD (and BPD). Consequently, the value of the *Tele2/Watson* judgment as a safety net to the IP Act and ECHR for the preservation of privacy in the digital age is limited by its scope of application. Perhaps, however, the ECtHR could emulate the CJEU's approach in *Tele2/Watson* as means of developing its own approach to proportionality and determining discretion in surveillance cases to better preserve privacy in the digital age.

1.5 Summary

In agreement with Cohen and Galic et al, it is concluded here that the participatory turn in the contemporary surveillance landscape has facilitated an extension of the state's surveillance reach with individuals' data exhaust being viewed as 'fair game'

---

[804] Ibid, para 127.
[805] Ibid, para 58.
[806] Ibid, para 119.
[807] *Parliament v Council* [2006] 3 CMLR 9. The IPT also considered this case of 'direct significance,' at para 34.
[808] Ibid, paras 58-59.

as opposed to being carefully considered in terms of the context within which it is shared and the expectations of privacy that persists in relation to that data.

Upon critical examination of the BCD and BPD powers under the ECHR and EU data protection law, it becomes clear that there has been a failure to critically assess the justifiability of extending the state's surveillance reach. Under the ECHR, it was shown that the proportionality of these powers was questionable in light of the severe consequences for both individual and societal interests in privacy. Although, it was acknowledged that a more substantive proportionality analysis might not be carried out by the ECtHR given the Court's tendency towards a more pragmatic assessment by focussing on the sufficiency of safeguards. Whilst *Szabo and Vissy v Hungary* could be indicative of an evolution in the ECtHR's determination of discretion in surveillance cases, as it stands, the Court's typical approach remains to focus on the sensitivity of data when determining discretion.[809] The danger of this approach in the contemporary surveillance landscape is that, states are potentially awarded too much discretion when it comes to the surveillance of data. As discussed above, data *about* a communication as opposed to its content is increasingly more revelatory, especially when aggregated in databases and subject to Big Data processes.[810] Accordingly, in order to preserve privacy in the digital age, the ECtHR may have to reconsider its focus and acknowledge the sensitivity of communications data in the contemporary surveillance landscape.

Finally, whilst the CJEU takes a more forthright approach to the assessment of proportionality in *Tele2/Watson* by listing a series of safeguards to be included in data retention legislation, the application of these principles would likely be limited to the retention powers in the IP Act. Consequently, this judgment fails to extend to the acquisition and use of communications data for national security purposes and, therefore, to provide a safety net for the protection of privacy against data-focussed powers slipping through the nets of the IP Act and the ECHR.

---

[809] See section 1.3 of this chapter (above).
[810] For risks of Big Data processing see Chapter 4, Part 2, section 1.2.3.

2 Outdated distinctions under Article 8 ECHR

This section examines the impact of the IP Act's failure to recognise the collapse of dichotomies on the protection of privacy in the digital age. This is achieved via an analysis of different safeguards applied to content and data-focussed powers in the IP Act under Article 8 ECHR. The content-data distinction examined in Chapter 4 thus provides the main focus of this discussion.[811]

It was concluded in Chapter 4 that data is differently intrusive as opposed to less intrusive and, as such, equally strong safeguards should apply to data-focussed surveillance powers.[812] The extent to which this is supported by the ECHR is established below. The following section first provides some background with a summary of the new oversight regime introduced by the IP Act.

2.1 Overview of oversight

David Anderson criticised RIPA for its inadequate system of oversight which he described as confusing, devoid of meaningful judicial involvement, and lacking in necessary independence from the state.[813] In light of such criticism, the IP Act significantly reformed the oversight of surveillance powers. One of the most prominent changes was the creation of the Investigatory Powers Commissioner ('IPC') to replace the three previous existing oversight bodies: the Interception of Communications Commissioner; the Chief Surveillance Commissioner, and; the Intelligence Services Commission.[814]

The IPC is supported by a team of Judicial Commissioners ('JCs') who hold or have held high judicial office and are appointed by the Prime Minister.[815] The IPC and his JCs provide judicial authorisation of powers that were previously only subject to

[811] See Chapter 4, Part 2, section 1.2.3.
[812] Chapter 4, Part 2, section 1.2.4.
[813] Anderson (n 158), para 2.86. All three of the reports published post-Snowden agreed that reform of the oversight regime under RIPA was required.
[814] IP Act 2016, s 227. Although David Anderson actually recommended the replacement of the three bodies with an 'Independent Surveillance and Intelligence Commission' ('ISIC') as opposed to just one commissioner.
[815] IP Act, s 227(2).

ministerial authorisation. For example, targeted interception,[816] targeted EI,[817] and all bulk warrants must now be approved by both the Secretary of State *and* a JC.[818] This is referred to as the 'double-lock' mechanism which is intended to provide

> '[d]emocratic accountability, through the Secretary of State, to ensure that our intelligence agencies operate in the interests of the citizens of this country, and the public reassurance of independent, judicial authorisation.'[819]

Other significant changes also include the creation of a new right of appeal from the IPT where an 'important point of principle or practice' arises, and the creation of additional requirements to be fulfilled before error-reporting or notification duties are carried out by the oversight bodies.[820] Whilst this represents an expansion of the IPT's powers, not all of Anderson's recommendations for enhancing the power of the IPT were adopted, including the extension of its jurisdiction to allow it to review errors made by services providers (as well as public authorities), and the ability to grant declarations of incompatibility.[821]

Whilst the consolidation of oversight duties into a single body under the IP Act is to be praised for its simplification of the unnecessarily complex system that previously existed under RIPA, serious concerns have arisen over: loopholes in the double-lock procedure; the lack of an adequate error-reporting and notification process; issues of accountability; and an over-emphasis on the 'human' examination of data. These issues are considered in greater depth below.

2.1 Applicable safeguards

This section establishes whether the ECtHR's general or strict safeguard principles apply to the content and data-focussed powers in the IP Act. The sufficiency of the

---

[816] Ibid, s 19.
[817] Ibid, s 102.
[818] Ibid, ss 138, 158, 178, 204(3).
[819] HC Deb 4 November 2015, col 972.
[820] IP Act, s 242(7)(a). This was recommended by Anderson (n 158) Chapter 14, para 14.105.
[821] Anderson (n 158) Chapter 14, para 14.103 and 14.106.

safeguards in the Act are subsequently assessed in terms of their fulfilment of these principles.

2.1.1 Content-focussed powers: interception and EI

As established in Chapter 2, the ECtHR applies stricter safeguards to interception powers to protect against arbitrariness.[822] These include: (i) categories of people likely to be subject to phone tapping; (ii) the nature of the offence likely to trigger the measure; (iii) judicially imposed limits on the duration of the interception; (iv) a prescribed method of summary reports; (v) procedures and safeguards for sharing material; (vi) procedures and safeguards for the destruction or erasure of material.[823] Only surveillance capable of disclosing 'information on a person's conduct, opinions or feelings' will demand the application of these stricter principles.[824] Otherwise, the more general principles will be applied by the ECtHR, which include: 'the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided for by the national law.'[825]

In light of the above, the stricter safeguard principles will apply to the interception powers in the IP Act. Furthermore, in *Bykov v Russia* it was held that the use of a radio-transmitting device was 'virtually identical' to interception and thus capable of triggering the stricter safeguard principles. On this basis, the stricter principles would also apply to EI powers given that they are 'virtually identical' to interception in terms of the 'nature and degree of intrusion involved.'[826] The sufficiency of the safeguards for interception and EI in the IP Act are thus assessed according to the ECtHR's stricter safeguard principles below.

---

[822] Chapter 2, section 2.1.4.1.
[823] *Kruslin v France* (n 262) para 33; *Huvig v France* (n 262) para 32. See further, Chapter 2, section 2.1.4.1
[824] *Uzun v Germany* (n 280), para 52.
[825] Ibid.
[826] *Bykov v Russia* App no.4378/02 (ECHR, 10 March 2009), para 79.

2.1.2 Data-focussed powers: data acquisition and retention, BCD and BPD

With regard to the data-focussed powers in the IP Act (acquisition and retention of communications data,[827] BCD and BPD) more careful consideration of the applicable safeguards is required in light of the differences in 'the nature and degree of intrusion involved.'[828]

In *RE v UK* it was held that the applicability of the stricter safeguard principles depends on the gravity of the interference as opposed to its technical definition.[829] This had the effect of extending the application of these principles outwith interception cases. As such, there is some scope to argue that the breadth of the data-focussed powers in the IP Act might still be capable of triggering the stricter safeguard principles. It is thus necessary to consider whether and at what point data-focussed powers could be considered analogous to interception in terms of their interference with privacy.

As argued in Chapter 4, changes in the way we now live our lives and advances in technological processing have rendered data-focussed surveillance significantly more intrusive than in previous eras with Big Data techniques enabling the identification of one's network, location history, habits, interests, religious and political affiliations.[830] The potential for processing that arises at the point of aggregation could thus be said to render the acquisition of communications data analogous to that of interception 'in terms of the nature and degree of the intrusion involved.'[831] In which case, the stricter safeguard principles ought to apply.

However, on the basis of *Bykov v Russia* (above) it is unlikely that data-focussed powers would be deemed 'virtually identical' to interception by the ECtHR. Despite being highly revelatory upon aggregation, these powers remain technically very different from interception and EI. Consequently, it is likely that only general safeguard principles would be applied to the data-focussed powers in the IP Act.

---

[827] Acquisition of communications data refers to the targeted version of BCD, see IP Act Part 3.
[828] Ibid.
[829] *RE v UK* (n 283) para 130. See Chapter 2, section 2.1.4.2.
[830] As noted by Dr Tom Hickman in his written evidence to the Joint Committee on the Draft IP Bill (IPB0039). See further Chapter 4, Part 2, section 1.3.1.
[831] *Bykov v Russia* (n 826), para 79.

Accordingly, it appears that the content-data distinction also pervades the ECtHR's approach to surveillance with weaker safeguards being applied to data-focussed powers on the (misguided) basis that content-focussed powers are more intrusive.

2.2 Sufficiency of safeguards

Having established the applicable safeguard principles above, this section assesses the sufficiency of the safeguards in the IP Act under Article 8 ECHR. Safeguards relating to content-focussed powers are examined against the stricter principles before examining the data-focussed powers against the general safeguard principles. This will enable any weaknesses in the protection of privacy caused by the content-data distinction in the IP Act to be demonstrated.

2.2.1 Interception and EI

This section assesses the sufficiency of interception and EI safeguards under the IP Act through the lens of *Zakharov v Russia* concerning the mass interception of communications by the state.[832] This case provides a recent and comprehensive analysis by the ECtHR on the types of safeguards required for the protection against arbitrariness and abuse of power in modern surveillance regimes. In addition, certain features of the Russian surveillance regime that the ECtHR took particular issue with are also found in the UK. This case therefore provides a strong foundation for conclusions to be made as to the sufficiency of safeguards in the IP Act. Although, given the tumultuous relationship between the ECtHR and Russia, the same conclusions may not be reached (or at least not to the same extent) in relation to the UK's surveillance laws.[833] The following aspects of the court's assessment of safeguards in *Zakharov* are examined below: (i) nature of offences; (ii) access and examination requirements; (iii) prior review and urgent procedure; (iv) categories of people; (v) notification requirements.

---

[832] *Zakharov v Russia* (n 204).
[833] See Lauri Malksoo and Wolfgang Benedek, *Russia and the European Court of Human Rights: the Strasbourg effect* (Cambridge University Press, 2017).

2.2.1.1 Nature of offences

The ECtHR has consistently maintained that whilst the foreseeability requirement does not require states to name the specific offences which may give rise to an interception, sufficient detail must be provided on the nature of offences capable of triggering secret surveillance acts.[834] In *Zakharov*, interception under Russian law could be carried out: (i) against those who had committed, were plotting, or were involved in a criminal offence punishable by over 3 years in prison; (ii) on those who may have information about a criminal offence or information relevant to the criminal offence; (iii) in the investigation of activities/events endangering Russia's national, military, economic, or ecological security.[835] The ECtHR took issue with the breadth of offences under Russian law capable of receiving a three-year prison sentence, meaning that minor crimes like pickpocketing, were capable of engaging interception.[836] It also noted the lack of clarification as to how the terms of (ii) might be applied in practice.[837] Finally, it held that whilst states are not compelled to list activities relating to national security, some indication must be given as to the degree of discretion awarded to the relevant authorities charged with determining what acts constitute a threat and whether it is serious enough to justify the surveillance in question.[838]

Under the IP Act, targeted and bulk interception and EI warrants may be issued where the Secretary of State considers it necessary on the grounds of preventing serious crime, national security, and in the interests of the economic well-being of the UK 'so far as those interests are also relevant to the interests of national security.'[839] The Secretary of State must also consider the proportionality of the warrant in pursuit of these legitimate aims.[840] Similar to Russia, a 'serious crime' under the IP Act are those incurring a prison sentence of three years or more.[841] In the UK, minor crimes (like pickpocketing) do not fall within this category meaning that the provision is

[834] See *Kennedy v UK* (n 308), para 159.
[835] *Zakharov v Russia* (n 204), para 244-248.
[836] Ibid, para 244.
[837] Ibid, para 245.
[838] Ibid, para 248.
[839] See for example, IP Act, s 178(2)(b).
[840] Ibid, s 178(c).
[841] Ibid, s 263(1).

considerably narrower in this regard.[842] However, this definition is widened by the subsequent inclusion of conduct: involving violence; resulting in financial gain; or, carried out by a large number of persons in pursuit of a common purpose.[843] Consequently, a large number of crimes are included in the definition of 'serious crime.' As Liberty previously warned regarding the use of this definition in RIPA, the common purpose head risks indiscriminately extending the scope of surveillance to include those engaged in legitimate collective activities, such as organised protests, who are not themselves party to any criminal activity.[844] Thus there exists some uncertainty over the scope of discretion awarded to the Secretary of State regarding what crimes are serious enough to justify the use of such invasive surveillance practices. In this respect, the interception and EI powers might fail to fulfil the foreseeability requirement under Article 8(2).

2.2.1.2 Access and examination

Further issues of discretion are also raised by the additional safeguard in place for the examination of information obtained under bulk interception and EI warrants. As discussed above, bulk warrants must set out specified 'operational purposes' for the human examination of material.[845] An operational purpose must relate to one or more of the statutory purposes specified on the warrant (eg it must relate to national security or the investigation of serious crime).[846] The 'list of operational purposes' is maintained by the heads of the intelligence agencies[847] and is reviewed by the ISC and Prime Minister.[848] Aside from this, there is very little guidance on what the list of

[842] For example, under s 22A of the Magistrates Courts Act 1980, low-value shoplifting (where the value of the stolen goods does not exceed £200) is punishable by a prison sentence not exceeding 6 months, or a fine, or both.
[843] IP Act, s 263(1). Same definition used in RIPA, s 81(3).
[844] RIPA Bill, Second reading briefing, Liberty, 28 February 2000. The courts are, however, sympathetic towards counter-terrorism and organised crime and recognise the challenges in policing and prosecuting them
[845] See for example, IP Act, s 142.
[846] *Operational case for bulk powers* (n 697), para 6.11.
[847] IP Act, s 142(4).
[848] Ibid, s 142(10).

operational purposes might actually include, leaving it unclear as to what types of events or activities might be considered a threat to national security or serious crime.[849]

As shown in Chapter 2, the headlines of discretionary powers must be included in primary legislation.[850] The Court can then take into account accompanying soft law when determining the extent to which an interference is foreseeable to individuals.[851] Thus, it is perhaps sufficient that the IP Act only states that the list of operational purposes is maintained by the heads of intelligence agencies and reviewable by the ISC and Prime Minister if accompanying soft law provides greater detail. However, aside from the explanatory notes stating that bulk warrants are likely to include a large number of operational purposes and that operational purposes must include more detail than the wording of one of the statutory purposes, little other information as to what an operational purpose might actually look like is provided.[852] On this basis, it might be argued that the IP Act fails to provide the individual with an adequate indication as to the circumstances in which public authorities are empowered to access and examine communications gathered under a bulk interception or EI warrant.

However, in *Zakharov* it was held that whilst Russian law failed to give 'any indication of the circumstances in which an individuals' communications may be intercepted on account of events or activities endangering Russia's national, military, economic or ecological security'[853] - (and thus left the authorities with a near unlimited degree of discretion in determining which events or activities constituted such a threat) – 'the existence of prior judicial authorisation served to limit the authorities' discretion.[854] On this basis, it is concluded that a similar judgment would be reached in relation to the examination of communications gathered under bulk interception and EI warrants in the IP Act. Whilst individuals remain fairly uncertain as to when such examination might occur, prior judicial authorisation works to limit the discretionary power granted

[849] As noted during the pre-legislative scrutiny of the IP Bill by Privacy International, see Privacy International written evidence (n 687), paras 43-45.
[850] Chapter 2, section 2.1.2.1.
[851] Ibid.
[852] *Draft Investigatory Powers Bill: explanatory notes* (n 843), para 382.
[853] *Zakharov v Russia* (n 204), paras 247-249.
[854] *Zakharov v Russia* (n 204), paras 247-249.

to the heads of the intelligence agencies. Although, as in *Zakharov*, the strength of this safeguard (prior judicial authorisation) must be examined in order to ensure that this discretionary power is meaningfully restricted.[855]

2.2.1.3 Prior judicial authorisation

In *Zakharov* the ECtHR held that the potential for arbitrariness arising from the broad discretion awarded to authorities could be offset by the requirement for prior judicial authorisation of warrants.[856] However, it also went on to find that the mere existence of a safeguard does not necessarily render it an effective one.

Similar to the IP Act, Russian law includes an 'urgent procedure' enabling interception to be implemented without judicial approval for up to 48 hours, failing which, the interception must cease immediately.[857] The ECtHR held that whilst urgent procedures are not inherently incompatible with Article 8,[858] too much discretion was awarded to Russian authorities to decide when this procedure could be used, creating significant opportunities for abuse of power.[859] In addition, the judiciary had no power to decide whether the material obtained during the urgent interception was kept or destroyed.[860] Consequently, the Court found that the safeguard of prior judicial authorisation was not capable of ensuring that secret surveillance measures were not used 'haphazardly, irregularly, or without due and proper consideration.'[861]

Under the IP Act, the Secretary of State can approve thematic and bulk interception and EI warrants in 'urgent cases' without the authorisation of a JC - thus constituting a significant loophole in the 'double-lock' mechanism.[862] The urgent procedure can also be used to carry out 'major modifications' of warrants[863] which enables the issuer

---

[855] Ibid, para 249.
[856] Ibid.
[857] Ibid, para 266.
[858] As seen in *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (n 321), paras 16 and 82.
[859] *Zakharov v Russia* (n 204) para 266.
[860] Ibid, para 267.
[861] *Zakharov v Russia* (n 204), paras 266-267.
[862] See IP Act, ss 25 and 109.
[863] See the urgent procedure for 'major modifications' of targeted and bulk interception warrants: IP Act, ss 38 and 147.

to add or vary the name and description of the person, organisation, or set of premises in the warrant.[864] Unlike the Russian system, urgent surveillance measures can operate for three (as opposed to two) days under the IP Act.[865] Furthermore, the definition of 'urgent' is left to the issuer who must believe there is an 'urgent need' for the procedure to be used.[866] No subsequent definition of 'urgent need' is provided in the Act. Before the end of the three days, the JC must decide whether to approve the warrant,[867] failing which the issuer must 'so far as is reasonably practicable' ensure that anything being done under the warrant stops as soon as possible.[868]

On the basis of *Zakharov*, this thesis concludes that the IP Act's definition of 'urgent' (or lack thereof), is not sufficiently clear and, therefore, fails to fetter the discretion of the issuer with regard to what constitutes an 'urgent need.' Consequently, there is a risk of arbitrary, irregular and improper use of these powers. This issue is worsened by the prohibition of JCs from judicially reviewing whether an 'urgent' situation did in fact exist.[869] This issue could be remedied by enabling the court to judicially review the use of the urgent procedure. For example, under the Counter-Terrorism and Security Act 2015 a court is required to judicially review the authorisation of 'urgent temporary exclusion orders.'[870] Where the authorisation is found to be 'obviously flawed,' the court can quash the order and must notify the individual concerned.[871]

2.2.1.4 Categories of people

Further issues of discretion arose in *Zakharov* regarding the categories of people likely to be subject to secret surveillance. Under Russian law, authorities could issue warrants authorising the interception of all communications in an area where an

[864] Ibid, s 34(5)(a). This is actually a reduced period from the Draft IP Bill which allowed urgent warrants to operate for 5 days (see Draft IP Bill 2016, s 20).
[865] Ibid, s 24.
[866] See IP Act, s 24(1)(b).
[867] Ibid, s 24(3)(a).
[868] Ibid, s 25(2).
[869] Ibid, s 25(8).
[870] Counter-Terrorism and Security Act 2015, schedule 5, s 3.
[871] Ibid, ss 4 and 5(2).

offence had been committed and need not necessarily state its duration.[872] In its assessment, the ECtHR underlined that an interception warrant

> 'must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered,' [–and that -] 'such identification may be by names, addresses, telephone numbers or other relevant information.'[873]

The Court went on to find that the discretion granted to Russian authorities regarding what communications where to be intercepted and for how long, was too broad.[874]

Given that thematic and bulk interception and EI warrants also fail to adequately establish the categories of people capable of being subject to these powers (as argued in section 2.2.1.1 above), a similar conclusion to *Zakharov* would also likely be reached in relation to this aspect of the IP Act.[875]

2.2.1.5 Notification requirements

The safeguards listed under Russian law were held by the ECtHR to be severely limited by the absence of notification requirements which effectively prohibited individuals from challenging the surveillance used against them.[876] The Court acknowledged that it might not always be feasible for subsequent notification in all cases as the threat against which the surveillance is being used might persist for years to come.[877] However, it went on to hold that as soon as notification can be carried out without frustrating the purpose of the surveillance, information should be provided to the subjects concerned.[878] Consequently, it was held that the Russian system which did not include any notification requirements, yet demanded proof of interception for

---

[872] *Zakharov v Russia* (n 204), para 265.
[873] Ibid, para 264.
[874] Ibid, para 265.
[875] As also held by the Joint Committee on the Draft IP Bill (n 670), paras 467-468.
[876] *Zakharov v Russia* (n 228) paras 286-287.
[877] Ibid, para 286.
[878] Ibid, para 287.

the individual's access to remedies, undermined the effectiveness of the law's remedies and safeguards.[879]

The above finding in *Zakharov* could support a similar conclusion in relation to the IP Act's lack of notification requirements and weaknesses in error-reporting provisions. Whilst the IPC must inform a person of any relevant error relating to them, the commissioner must: (i) consider the error a 'serious' one, and (ii) believe notification is in the public interest.[880] An error will not be a 'serious error' unless the IPC and IPT agree that it has caused 'significant prejudice or harm to the person concerned.'[881] The IP Act also states that a breach of a person's Convention rights, 'is not sufficient by itself for an error to be a serious error.'[882] Notification under the IP Act is, therefore, confined to a particularly onerous test regarding the seriousness of an error which even a breach of human rights may not satisfy. The high threshold for notification thus differs from the ECtHR's judgment in *Zakharov* where it held that a person ought to be notified as soon as is possible, as opposed to there being a presumption against notification.

Countering the above, however, is the ECtHR's judgment in *Kennedy v UK* where it was held that the ability of anyone to bring an action to the IPT, so long as they can show a public body has or may have acted in contravention of their convention rights, balances out these concerns over the lack of adequate notification requirements.[883] Therefore, given that the threshold for error-reporting under the IP Act is not applicable to persons applying to the IPT, a route to justice remains open to individuals. On this basis, it is unlikely that the lack of strong notification requirements would be deemed unlawful under Article 8(2) (or at least as fundamentally damaging to the effectiveness of the safeguards in the IP Act) by the ECtHR.

Although, in light of the discussion on autonomous machine analysis in Chapter 4, it is questionable how the individual would even be capable of suspecting that his or her

---

[879] Ibid.
[880] IP Act, s 231(1).
[881] Ibid, s 231(2).
[882] Ibid, s 231(3).
[883] *Kennedy v UK* (n 308), para 16.

convention rights had been interfered with by a program that can function independently of human input and, therefore, may be devoid of any human scrutiny or explanation.[884] Arguably, notification requirements could not even resolve this issue as no human might ever become aware of an injustice occurring. This raises questions about the role of the law within the contemporary surveillance landscape which is considered in Chapter 6.

2.2.2 Data acquisition, retention, BCD and BPD

This section examines the sufficiency of safeguards relating to data-focussed powers (the acquisition and retention of communications data, BCD, and BPD). As established above, these powers would likely only trigger the more general safeguard principles under the ECHR due to content being treated as more intrusive than data.[885]

2.2.2.1 Examination of data

As covered above, the government has defended bulk data-focussed powers on the basis that most of the data gathered will not be of intelligence interest and that electronic filtering will ensure that only data relating to the minority who *are* of interest will undergo 'examination.'[886] In other words, the majority of individuals make up the 'hay' and not the 'needles,' the latter of which is the real focus of intelligence analysts.[887] However, this does not mean that the privacy of the 'hay' is not interfered with in the search for a 'needle.'

'Examination of material' is defined in the IP Act as: 'material being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant.'[888] It follows that 'examination' can only be undertaken by a human who can read, look at, or listen to the material. Consequently, automated analysis of data is incapable of triggering the safeguards in place for the examination of material. For example, BCD warrants must state the 'operational purposes' for which the data collected can be

---

[884] See Chapter 4, Part 2, section 1.2.3.
[885] See section 2.1.2 of this chapter.
[886] *Operational case for bulk powers* (n 697) para 10.1. See further Chapter 4, Part 2, section 2.2.2.
[887] IP Act, ss 15(3) and 99(1)(b).
[888] Ibid, s 263(7).

selected for human examination. However, this means that prior to selection for examination, data can be electronically searched, filtered, and analysed without having to fulfil such a purpose.[889] Also, for the examination of domestic material obtained under a bulk interception or bulk EI warrant, a 'targeted examination' warrant is required.[890] However, prior to such human examination, data (both foreign and domestic) can be electronically searched without the need for further authorisation.

Regardless of the fact that the majority of individuals whose data is gathered has 'nothing to hide' in the eyes of the state, as argued in Chapter 4, there remain significant risks to their privacy (along with other rights such as freedom of expression and association) that occur long before a human 'examines' their data.[891] As set out in the introduction to this thesis, privacy is a multifaceted right that protects various aspects of individual and societal life.[892] Therefore, constructing it as a shield for wrongdoing used only by those with something to fear, serves to conceal its value and exclude from its protection the majority who are 'not of intelligence interest' from state over-reach.

Despite this, it is unclear whether the lack of a targeted examination warrant would fall short of the ECtHR's general safeguard principles.[893] Arguably, the ability to electronically search communications data and datasets without the need for a targeted examination warrant means that individuals are unable to foresee the circumstances in which their data will be processed in this way. The lack of notification requirements in the IP Act also means that they are unlikely to know whether their information has been electronically processed and what decisions have subsequently been made about them on the basis of this analysis.

It is thus concluded here that the lack of safeguards pertaining to the electronic analysis of data and datasets *should* be considered unlawful under Article 8(2). However, ultimately, this issue is dependent upon the ECtHR's opinion as to whether the use of

---

[889] IP Act, s 161(3).
[890] IP Act, s 15(3).
[891] See further Chapter 4, Part 2, section 1.3.1.
[892] See Introduction, section 2.
[893] See Chapter 2, section 2.1.4.2.

computer programs to search data constitutes an interference with Article 8(1). This question has been put to the ECtHR by Big Brother Watch in a Grand Chamber hearing on the bulk interception of external communications.[894] Upon publication of this judgment, it will be possible to reach a more concrete conclusion as to the sufficiency of the IP Act's safeguards in relation to the automated processing of data.

2.2.2.2 Request filter

The IP Act introduces 'filtering arrangements' for the searching of communications data, also referred to as the 'request filter.'[895] The 'request filter' was introduced as an additional communications data safeguard, available to all public authorities that enables them to search databases to identify relevant information in pursuance of an authorisation.[896] The Home Office thus views the request filter as a safeguard that filters out irrelevant information data and focusses searches. However, during the pre-legislative scrutiny of the IP Act, experts expressed serious concern over the ease with which public authorities are able to conduct complex searches of vast databases; noting in particular the risk of fishing expeditions on individuals and personal searches (for example, of an ex-partner) being carried out by analysts.[897]

However, there are some safeguards in place to prevent the abuse of the request filter. For example, the IP Act requires law enforcement to state the 'operational purpose' for accessing data through the filter.[898] In addition, the filtering arrangements are overseen by the IPC.[899] Therefore, despite the risks to privacy posed by the request filter, the relevant safeguards and oversight of the IPC would likely serve to fulfil the general safeguard principles under Article 8(2). This was also the conclusion reached by the Joint Committee on the Draft IP Bill.[900]

---

[894] *Big Brother Watch and Others v UK* 58170/13 (ECtHR, 4 November 2017).
[895] IP Act, ss 67-69.
[896] *Draft Investigatory Powers Bill: explanatory notes* (n 843) para 137.
[897] See, for example, the following written evidence to the Joint Committee on the Draft IP Bill: Dr Julian Huppert (IPB0130); LINX (IPB00097); Open Rights Group (IPB0108); Internet Service Providers' Association (IPB0137).
[898] IP Act, s 69(1)(b).
[899] Ibid, s 67(5).
[900] Joint Committee on Draft IP Bill (n 670) para 247.

2.2.2.3 Scope of BPDs

As set out above, BPDs are 'sets of information that includes the personal data relating to a number of individuals.'[901] Chapter 4 showed that the scope of BPDs was vague with examples ranging from the electoral register to financial data to social media data.[902] Due to the vague definition of BPDs, it remains unclear what information will be collected under this power and for what purpose. This led witnesses of the Joint Committee on the Draft IP Bill to advocate the specific exclusion of certain types of information from the scope of BPD (especially health records).[903] The Draft Code of Practice on BPD also does little to clarify the type of information collected under this power, merely reiterating that a BPD is a set of data obtained by an intelligence service including personal data on a host of individuals who are unlikely to be of intelligence interest.[904]

Consequently, the IP Act fails to provide the individual with sufficient clarity as to the scope and nature of BPD and grants too broad a discretion to the state with regard to what types of information can be collected under this power. On this basis, it is held here that the definition of BPDs would likely fall short of even the more general safeguard principles applied by the ECtHR.

2.2.2.4 Retention of communications data

As set out above, Part 4 of the IP Act permits the Secretary of State to order the retention of communications data by telecommunications operators for a period of up to 12 months.[905] Retention notices can be authorised for the investigation of non-serious crime and access to retained data can be authorised without prior review by a judicial or independent body. Following the *Tele2/Watson* case, Part 4 of the IP Act

---

[901] IP Act, s 199(1)(a)(b). N.b. s 199(1)(d) states that 'personal data' has the same meaning as in the DPA 1998 except it can also include information relating to a deceased person. See Chapter 4, Part 2, section 2.2.1.
[902] Ibid.
[903] Whilst additional safeguards were put in place for the health records, these were not excluded from the scope of BPD warrants (IP Act, s 206).
[904] Home Office, *Intelligence services' retention and use of bulk personal datasets: draft code of practice* (2017) para 2.2.
[905] IP Act, Part 4, s 86.

has been held incompatible with EU law by the Divisional Court on the basis that it fails to incorporate these safeguards.[906]

Whilst such explicit safeguards for the retention of communications data have not yet been prescribed by the ECtHR in its case law, it is arguable that a similar conclusion would be reached under Article 8(2); despite only the more general safeguard principles applying. This conclusion is reached on the basis that the retention of all communications data for purposes not restricted to the investigation of serious crime or national security fails to provide the individual with sufficient clarity as to the nature, scope and circumstances in which their data might be retained under the IP Act.

2.3 Summary

This section has served to demonstrate the impact of the outdated content-data distinction in the IP Act on the protection of privacy in the digital age. Based on the above analysis, it is concluded that the content-data distinction has led to a system of weak safeguards being applied to data-focussed powers due to data being viewed as less intrusive, as opposed to differently intrusive, than content. Although interception and EI safeguards fall down in some respects when assessed under the stricter safeguard principles, they are demonstrably stronger than those applied to the data-focussed powers. However, the above shows that the ECtHR also maintains a distinction between content and data, with weaker safeguard principles being applied to data-focussed surveillance powers. As a result, more scope exists for weaker safeguards to be deemed sufficient under Article 8(2) in relation to data-focussed powers. Although, even despite the application of the general safeguard principles to the data-focussed powers, the IP Act appears to fall short of this standard in a number of respects. Consequently, the Act is left highly vulnerable to future legal challenges and, indeed, already has been so challenged. In the meantime, privacy is left in a precarious position.

---

[906] *Liberty v SS for the Home Department* (n 782). See further section 1.4 of this chapter.

Conclusion

This chapter has critically assessed the impact of the IP Act's approach to the contemporary surveillance landscape on the protection of privacy in the digital age. This has been achieved via an analysis of the Act's response to the participation of the individual and the collapse of dichotomies under Article 8 ECHR. The ECtHR's own approach was also considered in terms of the extent to which it provided a safety net to the IP Act. Based on the above analysis, this chapter concludes with a list of findings on the suitability of UK surveillance law in the digital age.

First, the IP Act has successfully brought surveillance powers already used by LEAs and SIAs within the remit of the law. Previously, these powers were claimed by authorities under a variety of different pieces of legislation which created a complex and inaccessible surveillance law framework (as argued by Anderson, the ISC, and RUSI). Therefore, the IP Act takes a step towards bringing 'together all of the powers already available to SIAs and LEAs to obtain communications and data about communications.' This has helped to enhance the accessibility and foreseeability of surveillance powers used in the UK.[907] The IP Act has also drastically improved the oversight of surveillance powers by implementing a system of JCs. This is similar to the system proposed by David Anderson in 'A Question of Trust' although it is not an exact replica as Anderson had recommended the creation of an Independent Surveillance and Intelligence Commission ('ISIC') rather than just a group of JCs.[908] Nevertheless, in these respects, the IP Act provides a more comprehensive system of protection for privacy than under the previous surveillance law framework.

Second, it is concluded that the IP Act's haystack-needle approach fails to appropriately position the participation of the individual and has led to the introduction of disproportionate surveillance powers that infringe protected civil liberties, including: privacy, freedom of expression, freedom of association, and the prohibition of discrimination. Whilst this thesis acknowledges the serious risks to national security

[907] Home office, Secretary of State for the Home Department, *Investigatory powers bill: government response to pre-legislative scrutiny* (Cm 9219, 2016), para 7.
[908] Anderson (n 158) paras 14.47-14.57.

posed by global terrorism and serious crime – the uncertainty of which, acknowledges Zedner, ascribes a special value to information – it does not consider the mass surveillance introduced under the IP Act to be necessary, proportionate, or effective.[909] The following chapter therefore recommends the replacement of the bulk power regime with more restricted, targeted, versions of each in order to better reflect (and respect) the individual's ownership of surveillance brought about by the democratisation of (surveillance) technologies in the digital age. This is as opposed to the current approach which mistakenly interprets the individual's participation in digital data exchanges as a submission to the vertical gaze or antipathy toward privacy.

Third, despite collapsing dichotomies in the digital age, the IP Act is structured on the basis of dubious distinctions that results in inadequate protection of privacy from state surveillance. Despite the content of a communication being treated as more intrusive than its data under the IP Act, the Act still falls short of several of the stricter safeguard principles required under Article 8 ECHR for interception and EI powers. Regarding the data-focussed powers, it was acknowledged that greater scope exists for the IP Act's safeguards to fulfil the more general safeguard principles applied by the ECtHR. In light of this, it is concluded that the stricter safeguard principles should be applied to *all* of the bulk powers (not just interception and EI) given the significant risks to privacy posed by the mass aggregation and automated analysis of communications data illustrated in Chapter 4.[910] In this respect, the approach taken by the CJEU toward the retention of communications data in *Tele2/Watson* (where emphasis was placed on the *scale* of the surveillance rather than the *sensitivity* of the data) is preferred and recommended for adoption by the ECtHR in relation to the acquisition and use of communications data and personal datasets (given that these powers likely fall outwith the scope of EU law given their national security purpose).[911]

On the basis of the above, this chapter concludes that whilst there is a need to cast the surveillance net into the digital realm, there is also a need to set boundaries and

[909] Lucia Zedner, 'Why blanket surveillance is no security blanket' in Miller (n 16) 584-585.
[910] See Chapter 4, Part 2, section 1.2.3.
[911] As argued in section 1.4 of this chapter.

restrictions on its scope so that the individual is able to participate in contemporary society without forsaking all expectations of privacy. The IP Act successfully casts the net, but fails to respect protected waters. This stems from a failure to attune to the technocultural realities of the contemporary surveillance landscape which, in turn, results in a failure to preserve privacy in the digital age. The following chapter thus recommends ways to enhance the IP Act's approach to the third wave and, in turn, its protection of privacy.

Chapter 6 Recommendations and conclusions

Introduction

This thesis has argued that the IP Act has struggled to respond to the technocultural realities of the digital age, resulting in inadequate protection of privacy in the contemporary surveillance landscape. This conclusory chapter makes recommendations for change aimed at enhancing the law's protection of privacy and benefits bestowed on civil society by the third wave landscape.

In order for appropriate recommendations to be made, it is first necessary to establish the role of law in the contemporary surveillance landscape. It is unclear whether the law should be held entirely responsible for issues highlighted in this thesis and whether it should be looked to as the sole solution to the various dilemmas thrown up by the highly complex and diverse surveillance culture within which we now live.

Law-making in the digital age is fraught with difficulty. From the rate of technological change, to the borderless nature of the internet, to changing expectations of privacy (and surveillance); legislators face considerable challenges in striking the right balance between respect for individuals' privacy and the need to police cyberspace. This balance is a delicate and difficult one to strike as it requires the law to be precise enough that individuals are provided with a clear legal basis upon which to conduct their lives, whilst simultaneously retaining enough neutrality and breadth that it is not outmoded by surrounding technological developments.

The difficulty in striking the above balance must not be underestimated. Not only does it require law-makers to bridge the regulatory gap between 'realspace'[912] and cyberspace, but also to appease anxieties over global terrorist and crime networks (as well as other state actors) that now operate online. Therefore, perhaps this is too great a challenge to expect the law to deal with on its own, particularly given the slow pace

[912] As referred to by Andrew Murray, 'Internet Regulation' in David Levi-Faur (ed) *Handbook on the politics of regulation* (Edward Elgar, 2011) 267.

of lawmaking (relative to the pace of technological development) and the law's strong attachment to clear boundary-marking concepts which are increasingly being dissolved by borderless technologies.

In establishing the role of law in the contemporary surveillance landscape, three main models of internet regulation are considered: (i) cyberlibertarianism; (ii) cyberpaternalism; and, (iii) network communitarianism. After having provided an overview of each, network communitarianism is selected as the most relevant school of thought on the basis of the main themes of the contemporary surveillance landscape identified in this thesis, including: notions of victimhood and harm; expectations of privacy; the borderless-ness/fluidity/liquidity of modern surveillance; participation of the individual; and, group privacy. Recommendations for change are subsequently proposed that are in line with this model. This will ensure that the nuances of the third wave are reflected. Having proposed recommendations for change, this chapter identifies future areas for research, provides a final summary of the thesis, and finishes with concluding remarks.

1 The role of law in cyberspace

'The better laws can be made for the internet, the more autonomy and the better experiences people can have in their online lives.'[913] It is thus important to establish the role of law in order to propose recommendations for change that are appropriate for the digital age. After providing an overview of the three models of internet regulation listed above, it will be considered which theory is most appropriate in light of arguments presented in this thesis.

1.1 Cyberlibertarianism

In 1996, John Perry Barlow wrote the 'Declaration of Independence for Cyberspace' which formed the basis for cyberlibertarianism.[914] In the Declaration, Barlow declared

---

[913] Paul Bernal, *Internet privacy rights: rights to protect autonomy* (Cambridge University Press, 2014) 84

[914] John Perry Barlow, 'Declaration of independence for cyberspace' (*Electronic Frontier Foundation*, February 8 1996) <https://www.eff.org/cyberspace-independence> accessed 16 February 2018. The declaration was written as part of an online event called the '24 hours in cyberspace project' which was an online even that aimed to create a digital time capsule of online life.

that the internet is immune from government sovereignty for two reasons: (i) users have not consented to being governed and so there is no social contract providing a legitimate basis for government rule online; and, (ii) government cannot control the actions of individuals online due to the borderless nature of the internet which renders traditional legal enforcement procedures obsolete.[915] Accordingly, cyberlibertarians advocate self-regulation online, arguing that only the internet community are capable of, and should be responsible for, creating and enforcing the norms of cyberspace.[916] Indeed, Chapters 4 and 5 show that UK lawmakers have struggled to grasp the issues presented by ICTs and the nature of individuals' engagement with them. The UK surveillance legal landscape thus supports the cyberlibertarian argument in so far as it demonstrates the law's struggle to respond to challenges presented by the technocultural realities of the digital age.

However, cyberlibertarianism is widely criticised on the basis that laws have successfully been made for the internet. Also, regarding the social contract argument, Murray argues that cyberlibertarianism reflects a very narrow view of legitimacy which fails to recognise other views on relationships between government and the governed.[917] Furthermore, Goldsmith argues that the foundation of cyberlibertarianism (that the non-geographical nature of cyberspace renders legal enforcement futile), is rooted in a 'nineteenth century territorialist conception' of law which has since been replaced by the courts' application of 'universal customary laws tied to no particular sovereign authority, such as the law merchant, the law maritime, and the law of nations.'[918] From such criticism of cyberlibertarianism, was born the cyberpaternalism model of internet regulation predominantly led by Reidenberg and Lessig.[919]

---

[915] Barlow, ibid. Barlow's arguments were also developed in David Johnson and David Post, 'Law and borders: the rise of law in cyberspace' (1996) 48 Stanford Law Review 1367.
[916] Johnson and Post, ibid, 1388-89.
[917] Murray (n 912) 271.
[918] Jack Goldsmith, 'Against cyberanarchy' (1998) 65 Chicago Law Review 1199, 1206-1207.
[919] Joel Reidenberg, 'Lex informatica: the formulation of information policy rules through technology' (1998) 76 Texas Law Review 1439; Lawrence Lessig, 'The new Chicago School' (1999) 27 Journal of Legal Studies 661, and Lawrence Lessig *Code and other laws of cyberspace* (Basic Books, 1999).

1.2 Cyberpaternalism

At the heart of this school is the marrying of law and technology to establish effective regulation and enforcement procedures online, such as laws requiring technology to be built in such a way that they prohibit certain activities from being carried out (see examples below). Reidenberg refers to this concept as 'lex informatica.'[920] Lessig built on Reidenberg's work to develop his theory on 'the New Chicago School.'[921]

Lessig argues that under 'the Old Chicago School' the individual is worked on by four modes of regulation ('modalities'): (i) laws, which direct behaviour by threatening sanctions; (ii) norms, which are enforced by a community; (iii) markets, which regulate through price, and; (iv) architecture, which physically prohibits actions (see figure 1).[922] These four modalities work to guide the behaviour and actions of the individual (regulatee) in such way that she is reduced to a 'pathetic dot' (as shown in Figure 1, below).

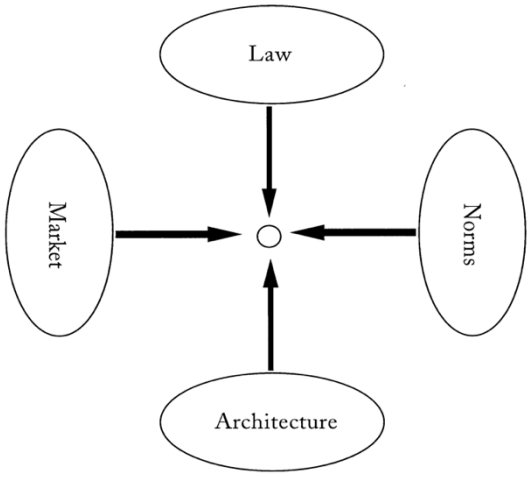

Figure 1: Source: Lawrence Lessig, 'New Chicago School' (1999), p 664

Under the 'New Chicago School' Lessig argues that the law is not displaced by these other types of regulation; rather, the law regulates the other modalities – either directly via the use of traditional means to direct an object of regulation, or, indirectly by regulating the other regulators (see Figure 2, below).[923] He gives the example of a

[920] Reidenberg (ibid).
[921] Lessig, 'The new Chicago school' (n 919).
[922] Ibid, 662-663.
[923] Ibid, 666.

government trying to reduce smoking: laws may be passed banning cigarettes or imposing restrictions (such as a minimum age for purchase); or, the law could increase the price of tobacco products (the law regulating the market); or, the law could fund an anti-smoking campaign to influence public opinion (the law regulating social norms); or, the law could regulate the nicotine in cigarettes (the law regulating the architecture of cigarettes).[924] Lessig thus underlines the importance of seeing regulatory tools together, rather than distinct or separate from one another, in order to achieve the desired regulatory effect.

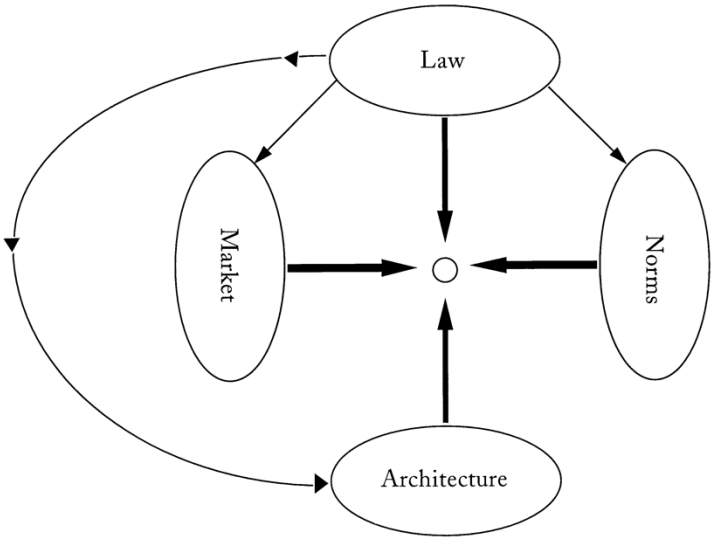

Figure 2: Source: Lessig, 'The New Chicago School,' p 667

In 'Code and Other Laws of Cyberspace' Lessig applies the 'New Chicago School' to the internet.[925] He argues that the architecture of cyberspace, differs from that of 'realspace' as it does not pre-exist. Rather, we design and construct the architectures we desire via code meaning that

> 'we can build, or architect, or code Cyberspace to protect values that we believe are fundamental, or we can build, or architect, or code Cyberspace to allow these values to disappear.'[926]

[924] Ibid, 667-668.
[925] Lessig, *Code and other laws of cyberspace* (n 919).
[926] Ibid, 6.

Accordingly, laws are not obeyed out of obedience or morality but because the option not to obey is made technically impossible. For example, regarding privacy protection online, Lessig argues that the law should be used to 'tame code' so that individuals are provided with opportunities to exercise choice over their privacy,[927] for which he recommends the use of a 'Platform for Privacy Preferences' (also known as 'P3P').[928]

Under a P3P regime, machine-readable privacy policies are used to alert individuals to a conflict between a website and their privacy preferences, thus enabling the individual to 'express their preferences and negotiate the use of data about them.'[929] Whilst Lessig does not go as far as endorsing the adoption of P3P, he uses it to illustrate

> '[a]n architecture, tied to a market, that protects privacy rights in a way that real space cannot, but that architecture will not emerge on its own. It needs the push of law.'[930]

Lessig therefore looks to the state to step in and create space for the individual to exercise control over their data.[931] He also seeks to bridge the cyberlibertarian gap between 'realspace' and cyberspace, challenging the cyberlibertarian construction of the latter as immune from realspace regulation by depicting code as a 'perfect technology of justice.'[932] In line with Raab and de Hert's argument that regulation for cyberspace is a 'social and political process' involving various different actors and institutions, Lessig's theory acknowledges that law is not the only existing regulatory instrument and that the regulation of cyberspace demands a combination of these modalities to achieve the desired outcome.[933] Whilst the other modalities do not displace law, they can be subject to it, enabling the law to regulate behaviour indirectly

---

[927] Ibid, 514-521.
[928] Ibid, 160.
[929] Ibid.
[930] Ibid.
[931] Reidenberg similarly discusses the 'complex mix' of mechanisms for privacy regulation, see Reidenberg (n 919) 96. Andrew Murray and Colin Scott also recommend a focus on hybrid models of regulation in, 'Controlling the new media: hybrid responses to new forms of power' (2002) 65 MLR 491.
[932] Lawrence Lessig, 'The zones of cyberspace' (1996) 48 Stanford Law Review 1403, 1408.
[933] Charles Raab and Paul de Hert, 'Tools for technology regulation: seeking analytical approaches beyond Lessig and Hood,' in Roger Brownsword and Karen Yeung (eds) *Regulation technologies: legal futures, regulatory frames and technological fixes* (Hart publishing, 2008).

as well as directly.[934] Lessig is praised for opening 'the eyes of many in the legal profession by challenging the law's classical self-understanding that narrows regulation to a question of making laws.'[935]

However, his application of the 'New Chicago School' to privacy protection (particularly regarding his P3P proposal) has been criticised for positioning consent as 'the linchpin for protecting privacy' and, therefore, conceptualising privacy as a property right.[936] Schwartz argues that the success of Lessig's privacy protection is dependent upon the creation of a satisfactory interface that enables the individual to exercise effective control over their personal information.[937] The design of such an interface is incredibly difficult and complex. It also requires 'simplifications and glosses to be made,' which might

> '[f]acilitate trading personal information on bad terms, but, more broadly, will shift power to those who decide how important shortcuts are to be taken,' [– and so –] 'property plus code may turn into a powerful means for generating an unsatisfactory level of privacy.'[938]

However, in defence of his conceptualisation of privacy as property, Lessig argues that his theory recognises that privacy is valued differently by different people and, as such, allows the individual to ascribe his or her own value to privacy.[939] Certainly, as shown in this thesis, there are a variety of different expectations of privacy that exist in the current surveillance landscape, with some desiring exposure whilst others seek anonymity. 'Privacy as property' could, therefore, offer a way in which these differences are respected without the law having to delve into the specifics of how

---

[934] Lessig, 'The new Chicago school,' (n 919), 672.
[935] Raab and de Hert (n 933), 265.
[936] Ibid, 267
[937] Paul Schwartz, 'Beyond Lessig's code for internet privacy: cyberspace filters, privacy control, and fair information practices' (2000) Wisconsin Law Review 243.
[938] Schwartz, ibid, 277. For other criticism of Lessig's 'privacy as property' notion see: Mark Lemely, 'Private property' (2000) 52 Stanford Law Review 1545; Mark Rotenberg, 'Fair information practices and the architecture of privacy: (What Larry doesn't get)' (2001) 1 Stanford Law Review 89; Julie Cohen, 'DRM and privacy' (2003) 18 Berkeley Technology Law Journal 575.
[939] Lawrence Lessig, *Code version 2.0* (Basic Books, 2006) 228-229.

each individual experiences different online environments and contexts. In further defence of his theory, Lessig argued that privacy protection would be strengthened

> '[i]f people conceived of the right as a property right. People need to take ownership of this right and protect it, and propertizing is the traditional tool we use to identify and enable protection.'[940]

For reasons listed by Schwartz, above, this thesis does not endorse Lessig's conceptualisation of privacy as property. However, it *does* agree with the cyberpaternalist school of thought insofar as a hybrid regulatory model is required for the effective regulation of cyberspace and that code can at least play a role in the protection of privacy by removing opportunities to breach laws. Although, what such an architecture might look like is unclear.

1.3 Network communitarianism

Network communitarianism was developed in response to cyberpaternalism, challenging its apparent failure to 'account for the complexities of information flows found in a modern telecommunications/media system such as the internet.'[941] In agreement with cyberlibertarianism, network communitarians recognise the strength of internet users, although they do not go as far as arguing that cyberspace should be left to self-regulate, thus agreeing with Lessig that 'laissez-faire will not cut it.'[942] Therefore, this school takes up something of a middle ground between the two extremes of cyberlibertarianism and cyberpaternalism. This is illustrated by Murray's theory of the 'post-regulatory (cyber) state.'[943]

---

[940] Lessig, ibid, 229.
[941] Andrew Murray, *Information technology law: the law and society* (3rd edn, Oxford University Press, 2016), 71
[942] Lessig *Code 2.0* (n 27), 232
[943] Andrew Murray, 'Conceptualising the post-regulatory (cyber) state' in Brownsword and Yeung (n 933). He develops this theory on the basis of previous work on the 'post-regulatory state,' including: Colin Scott, 'Regulation in the age of governance: the rise of the post-regulatory state' in David Levi-Faur (ed) *Handbook on the politics of regulation* (Edward Elgar, 2011); Julia Black, 'Decentring regulation: understanding the role of regulation and self regulation in a 'Post-Regulatory' world' (2001) 54 Current Legal Problems 103.

Murray's theory maintains that within the digital age, 'the reach of regulators is restricted: the reach of technology is global.'[944] In the 'post-regulatory (cyber) state' a person is able to use alternative outlets to overcome undesirable aspects of the prevailing regulatory matrix being applied to them.[945] For example, if someone wants to watch a movie that has not yet been released in their country, they can go online and stream the content from a website. Thus, individuals are able to change aspects of the online environment or 'architecture' in order to pursue a particular desire. This leads Murray to the position that the flexibility and uncertainty of the technological landscape condemns static models of internet regulation to failure.[946]

However, Murray is careful to distinguish his concept of the 'post-regulatory (cyber) state' from the traditional cyberlibertarian school of thought (which he does not consider supportable today) by describing his theory as 'cyberlibertarianism 2.0'[947] Murray maintains that 'cyberlibertarianism 2.0' does not mean that external regulation will never be effective unless supported by the community, but that adequate consideration *must* be given to the flexibility of the technological landscape and the power of the network.[948]

To demonstrate the strength of the online network, Murray develops Lessig's theory on the 'pathetic dot' into a 'networked matrix of active dots,' where

> 'the individual dot is part of a complex community of dots who through Information and Communication Technologies are empowered to gather and communicate more perfectly as individuals than at any time in our history (and it is fair to assume this ability will continue to grow and develop).'[949]

---

[944] Murray, ibid, 295.
[945] Ibid, 294.
[946] Ibid, 295.
[947] Ibid, 296.
[948] Ibid.
[949] Ibid, 301.

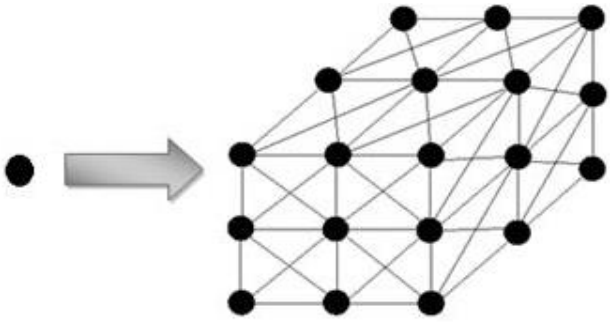

Figure 3: Source: Murray, 'Internet regulation' (2011), p 285

Accordingly, Murray argues that 'the regulatory process is in nature a dialogue not an eternally imposed set of constraints.'[950] Thus, within the active matrix the individual is not a pathetic dot worked on only by regulators, but rather, part of a regulatory matrix capable of affecting regulation. In support of this he gives the example of pornography no longer being prosecuted under the Obscene Publications Act 1959 as the community of dots have shown via their consumption of this material online that its viewing is no longer morally objectionable.[951]

Given that the actions of each dot can affect change within the regulatory environment, forming a regulatory model for the 'post-regulatory (cyber) state' is significantly more complex than regulating for the physical realm which is considerably more stable and predictable.[952] However, noting the success of previous regulations in cyberspace, Murray does not take up a cyberlibertarian position by deeming the post-regulatory (cyber) state as unregulable.[953] Rather, he argues that it demands a re-think of the roles of the regulator which is no longer just to regulate and control a 'passive collective.'[954] This 'passive collective' no longer exists and the dot is no longer 'pathetic' as it is capable of determining the success of a regulation.[955] Thus, under network

[950] Murray (n 843) 285.
[951] Ibid, 286. Clearly this excludes certain types of pornography that are still deemed morally objectionable by society and, thus, are still illegal.
[952] Murray (n 943) 301.
[953] Ibid 302.
[954] Ibid 303.
[955] Ibid 302.

communitarianism, the roles of the regulator and regulatee are merged, with both being capable of regulating and being regulated on.

In light of the above, Murray proposes the following three-stage process for regulating in the post-regulatory (cyber) state: (i) develop a dynamic model of the environment surrounding the action the regulator wishes to regulate; (ii) design a regulatory intervention that harnesses the communication flows of the pre-existing regulatory matrix to encourage the uptake of the regulatory intervention; (iii) test the regulatory intervention thoroughly via constant monitoring of feedback and make changes accordingly.[956] This regulatory process, argues Murray, is key to the creation of 'effective, symbiotic, regulatory interventions' within the post-regulatory (cyber) state.[957]

Having provided an overview of the main regulatory models for cyberspace, it is now necessary to determine the most appropriate model for regulating in the contemporary surveillance landscape and, on this basis, to suggest recommendations for change that will work towards resolving the issues raised in this thesis.

2 The role of law in the third wave landscape

First, with regard to cyberlibertarianism; whilst this thesis acknowledges the strength of the online community, it does not endorse the conception of cyberspace as 'elsewhere' and therefore immune from law. As shown above, Goldsmith deftly attacks each of the premises upon which this notion is predicated.[958] In particular, this thesis does not agree that the borderless nature of the internet negates the legitimacy of real world regulations which can, and indeed have, been adapted and developed to overcome this challenge. For example, it *could* be argued that the introduction of bulk surveillance powers by the IP Act responds to the Internet's defiance of geography and facilitation of transnationalism by removing the limits of surveillance to emulate the

[956] Ibid 315.
[957] Ibid.
[958] Goldsmith (n 918).

borderless nature of life within the digital era.[959] Whilst this thesis does not endorse this approach, it arguably demonstrates that the law has attempted to adapt and develop in order to overcome the increasingly invisible horizon of the digital landscape. Finally, in relation to cyberlibertarianism, this thesis agrees with Lessig that 'the legitimacy of regulation turns upon its effects,' and as such, the internet is a legitimate subject of regulation given its ability to have significant effects in realspace.[960] For these reasons, this thesis agrees with cyberpaternalists and network communitarians that traditional cyberlibertarianism is not supportable today.

Second, regarding cyberpaternalism; in 'Code 2.0' Lessig identifies two threats to privacy posed by the internet: (i) threats from digital surveillance, namely the growing capacity of government to spy on activities, and (ii) threats from the increasing aggregation of data by private entities for commercial purposes.[961] He argues that the four modalities (law, norms, market, and architecture) represent four types of response to these threats and that the answer lies in not one, but at least two of these regulatory forms.[962] In relation to digital surveillance, he argues that the law should only sanction such practices where certain conditions are fulfilled, such as, a description of the purpose for which an algorithm is used and the requirement of judicial review for action to be taken against an individual on the basis of the algorithm.[963] He argues that such laws should also be accompanied by architectural regulation such as 'privacy enhancing technologies' ('PET') that enhance anonymity online (eg the P3P regime).[964] Whilst P3P has not been widely implemented, it represents Lessig's general response to privacy problems posed by cyberspace, that

---

[959] 'Transnationalism' defined as 'the processes by which immigrants forge and sustain multi-stranded social relations that link together their societies of origin and settlement' in Linda Basch, Nina Schiller, Cristina Blanc, *Nations unbound: transnational projects, postcolonial predicaments and deterritorialized nation-states* (Routledge, 1994) 8. Baldassar later notes that the role of the internet in transnationalism, see Loretta Baldassar, 'Home and away: migration, the return visit and "transnational" identity' in Ien Ang and Michael Symonds (eds) *Home, displacement, belonging, communal/plural 5* (NSW Research Centre in Intercommunal Studies, 1997) 74.
[960] Lessig, 'Zones of cyberspace' (n 932) 1404-1405.
[961] Lessig, *Code 2.0* (n 939) 223.
[962] Ibid, 223.
[963] Ibid, 224.
[964] Ibid, 226.

> '[w]e must build into the architecture a capacity to enable choice – not choice by humans but by machines…machine-to-machine negotiations about privacy so that individuals can instruct their machines about the privacy they want to protect.'[965]

Cyberpaternalism is attractive because it confronts the complexities of regulating for cyberspace without undermining the value of law in this realm. Thus, in agreement with this thesis, the law remains relevant but needs to attune to the technocultural realities of the digital age in order to provide adequate protection of privacy. Cyberpaternalism effectively carves out a space for law in cyberspace by enhancing its strengths via other modalities, such as code (architecture). However, as discussed above, this school of thought fails to appreciate the ability of individuals to affect regulatory change, reducing them to a 'pathetic dot' controlled by regulators as opposed to a constituent of an active matrix capable of affecting regulatory change. Thus, in agreement with Raab and de Hert,

> '[t]he work of Lessig needs to be augmented by more general approaches that emphasise and demonstrate empirically the multiplicity of relationships and pathways among a larger number of tools, and that map the tools onto a cast of characters involved in the regulatory process.'[966]

For this reason, this thesis considers network communitarianism to be the most appropriate regulatory model for the current, third wave landscape where individuals are active participants in surveillance, capable of setting, establishing, and overturning surveillance norms and regulations.[967] Support for this conclusion and the ability of 'the dots' to determine the fate of regulation is demonstrated by the following analysis of the Draft Communications Data Bill 2012.

---

[965] Ibid, 232.
[966] Raab and de Hert (n 933), 282.
[967] As argued by Paul Bernal (n 913), 84.

2.1 The Draft Communications Data Bill 2012

The Draft Communications Data Bill 2012 (nicknamed the 'Snooper's Charter') sought to ensure the availability of communications data and its acquisition by public authorities. The Bill faced significant opposition from civil liberties organisations, communication service providers ('CSPs'), and the general public – as shown in the highly critical report of the Joint Committee on the Draft Communications Data Bill.[968] Significant controversy arose over the sweeping powers granted to the Secretary of State allowing her to require that communications data be made available to public authorities by telecommunications operators.[969] The following aspects of the power were especially contentious: the only limitation on what communications data should be made available was that it be 'necessary' (for which no definition was provided);[970] communication service providers might have to generate data not already collected by them;[971] the data must be retained for 12 months;[972] and, the data was available to a long list of public authorities (which could be added to by order).[973] The government defended the breadth of the power by maintaining that there was no intention to use it fully, maintaining that it was a way of future-proofing the law by ensuring that any new types of communications data fell within its scope.[974] However, the report of the Joint Committee on the Draft Communications Data Bill concluded that such a precautionary approach to law-making did not justify such a wide power. Instead, it recommended that such laws relating to the internet be reviewed and updated regularly as opposed to being drafted so loosely.[975] Other controversial aspects of the bill included: the power to collect web logs (similar to the power to acquire 'Internet Connection Records' under the IP Act, website addresses up to the first '/' were to be gathered by internet providers);[976] a broad definition of communications data;[977]

---

[968] Joint Committee on the Draft Communications Bill, *Draft Communications Data Bill* (2012-13, HL 79, HC 479).
[969] Draft Communications Data Bill 2012, s 1.
[970] Ibid, s 9(1).
[971] Ibid, s 17(1).
[972] Ibid, s 4(1).
[973] Ibid, s 21(1)(e)
[974] Ibid, para 66.
[975] Ibid, para 70.
[976] Draft Communications Data Bill 2012, s 28(4).
[977] Ibid, s 28(1).

extraterritorial reach;[978] broad access powers to public authorities.[979] In light of these issues and strong opposition to the bill, Deputy Prime Minister Nick Clegg stated in a radio interview that 'what people have dubbed the Snooper's Charter' was 'not going to happen.'[980]

Bernal uses the example of the Draft Communications Data Bill 2012 to support the viability of network communitarianism as an appropriate regulatory model for the current landscape.[981] He proceeds on the basis that the active community of dots were successful in determining the fate of the Bill which lacked the necessary legitimacy to successfully intervene in the pre-existing regulatory matrix. However, the provisions of the 2012 Bill did eventually come to fruition, albeit fragmentally, via subsequent pieces of legislation. Renewed interest in the Bill was sparked by the terrorist attacks at the offices of French magazine 'Charlie Hebdo' in 2015, with the Home Secretary indicating that an amended version would be introduced at the earliest opportunity.[982] Despite opposition from the Liberal Democrats and Scottish National Party, the 2015 Queen's Speech included an undertaking that new legislation would be introduced to modernise the law on communications data.[983] This eventually took the form of the IP Act which has introduced many of the powers originally introduced under the 2012 Bill.

However, even prior to the passing of the IP Act, some of the provisions of the 2012 bill had already been enacted via other pieces of legislation. Under DRIPA 2014, for example, the Secretary of State was able to require the retention of communications data by public telecommunications operators.[984] Part 3 of the Counter-Terrorism and Security Act 2015 also amended DRIPA 2014 to enable the Secretary of State to

---

[978] Under Part 1 of the 2012 Bill communications data could be requested from overseas providers. For discussion of extraterritorial issues surrounding this power see *Joint Committee on the Draft Communications Data Bill 2012 Report* (n 968), Chapter 6 Jurisdictional Issues.
[979] Ibid, s 5.
[980] Deputy PM Nick Clegg speaking on his weekly 'Call Clegg' phone-in on LBC 97.3 Radio.
[981] Bernal (n 900) 84.
[982] See Philip Ward, *Briefing paper: Communications data: the 2012 draft bill and recent developments* (No.06373) (House of Commons Library, 12 June 2015), 3.
[983] Prime Minister's Office, 'The Queen's Speech 2015' (27 May 2015) <https://www.gov.uk/government/speeches/queens-speech-2015> accessed 5 June 2018.
[984] DRIPA, s 1.

require Internet Service Providers ('ISPs') to retain data allowing authorities to identify the persons or device using a particular IP address at a specific time (which had also been a provision of the 2012 Bill).[985] Therefore, by adopting a more fragmentary approach to law-making, there was a 'creeping' actualisation of provisions which, when introduced in 'whole' form, had previously been deemed unacceptable.

The 2012 Bill questions the viability of network communitarianism as the most appropriate regulatory model for the current surveillance landscape as its provisions were ultimately pushed through via subsequent laws. This could be used to argue that the 'dot's' ability to affect regulators is limited and, therefore, indicative of a regression back to cyberpaternalism where the individual is little more than a 'pathetic dot' worked on by regulators.

Alternatively, it could be argued that it is simply more difficult to keep track of several draft bills at once. It might also be argued that the Charlie Hebdo attack in Paris and the terrorist murder of Fusilier Lee Rigby in London caused a societal and governmental re-think of the necessity and proportionality of more aggressive surveillance powers. This is supported by the briefing paper 'Communication Data: The 2012 Draft Bill and Recent Developments,' which demonstrates renewed interest in the 2012 Bill following the Charlie Hebdo attacks by MI5, the PM and Deputy PM, the Home Secretary and the Labour party.[986] Although, residual resistance to the 2012 Bill remained with Lord King's proposed amendments to the Counter Terrorism and Security Bill 2015 being rejected on the basis that they aimed to re-introduce the 'Snooper's Charter.'[987] A 'YouGov' poll for the Sunday Times taken after the Hebdo attack also found that the British public were supportive of increasing the security services access to public communications in order to fight terrorism (by 52% to 31%).[988] 53% also voted that phone and internet companies should retain everyone's

---

[985] Counter-Terrorism and Security Act 2015, s 21.
[986] Philip Ward (n 982).
[987] Ibid, section 6.5, p 20.
[988] Will Dahlgreen, 'Broad support for increased surveillance powers' (*YouGov*, 18 January 2015) <https://yougov.co.uk/news/2015/01/18/more-surveillance-please-were-british/> accessed 5 June 2018.

internet browsing history, emails, voice calls, social media interactions, and mobile messaging, which could then be accessed for anti-terrorism purposes.[989]

2.2 Summary

In light of the above evidence, it is argued that the dot remains part of an active matrix capable of effecting regulatory change. As shown above, Murray specifically distinguishes network communitarianism from the traditional cyberlibertarian approach in that he does not advocate self-regulation, but rather, calls for the acknowledgment of the ability of regulators and regulatees to regulate. This does not mean that regulatees cannot be worked on or 'pulled to compliance' by regulators.[990] The eventual passing of the Communications Data Bill 2012, albeit in fragmented form, can thus be seen as a result of interaction between regulators and regulatees, the latter of which had to be managed in order for provisions of the bill to eventually be deemed legitimate by the 'matrix of dots.'

This thesis, therefore, endorses network communitarianism as the most appropriate model for regulating cyberspace. This is in agreement with other scholars like Paul Bernal, who also view network communitarianism as the regulatory model closest 'to the reality of the internet as it currently exists.'[991] Raab and de Hert similarly praise Murray's regulatory theory as, 'a particularly useful development of regulatory analysis that emphasises the need to identify actors active within multi-regulatory regimes.'[992] On this basis, the following section harnesses Murray's network communitarianism approach by proposing recommendations aimed at improving the law's understanding of the individual's (active) role in the digital age. This is intended to enhance the legitimacy of surveillance laws and pull individuals toward compliance. The following section also underlines the need for engagement with other disciplines and complementary non-legal regulatory tools to be used alongside the law, thus

[989] Ibid.
[990] For discussion on the 'pull to compliance' see Thomas Franck (n 65).
[991] Bernal (n 913) 83-84.
[992] Raab and de Hert (n 933) 281.

fulfilling Murray (and Lessig)'s call for dynamic and hybrid regulations for cyberspace.

3 Recommendations for change

With Murray's network communitarian approach in mind, the following recommends ways in which the UK surveillance legal landscape could become more attuned to the technocultural realities of the contemporary surveillance landscape and, therefore, provide more adequate protection to privacy in the digital age. This section is structured as follows: (i) re-constructing dichotomies; (ii) re-positioning participation; and, (iii) recognising the group.

3.1 Re-constructing dichotomies

Chapter 4 showed that UK lawmakers have struggled to move away from traditional boundary-marking concepts, continuing to enforce distinctions that lack relevancy within the current technological environment. The content-data distinction was used to illustrate the impact of this failure on the protection of privacy in the digital age. It was shown that the distinction resulted in significantly weaker safeguards being applied to data-focussed powers compared with the content-focussed powers of interception and EI.[993] The content-data distinction was also shown to indicate the IP Act's maintenance of a highly spatial, public-private dichotomy,[994] the danger of which lies in the law's subsequent failure to recognise the permeability of the boundary between public and private space (and information) in the digital age and to accord subsequent protection to privacy outwith traditionally private spaces like the home.[995]

In light of these findings, this section considers how best to approach boundaries in 'a technology pervaded world in which space, self, and society increasingly collapse.'[996] Discussion is focussed mainly on developing the public-private dichotomy. By re-adjusting the law's delineation of the 'public' and the 'private,' it is argued that other problematic distinctions present in UK surveillance law will also be improved,

[993] See Chapter 5, sections 2.1 and 2.2.
[994] See Chapter 4, Part 2, section 1.2.3.
[995] This 'permeability' was discussed in Chapter 3, Part 2, section 1.2.2.
[996] See further Chapter 3, Part 2, section 1.2.2.

especially the content-data distinction which flows from a conception of the 'inside' being more private than the 'outside.'[997]

3.1.2 Re-conceptualising privacy

The law is the primary tool for setting boundaries. In doing so, individuals are able to regulate their behaviour and actions according to what they should or should not do in certain circumstances. The home has traditionally been viewed as the epitome of private space worthy of the highest legal protection. However, this thesis has shown that such spatial conceptions of privacy are becoming increasingly difficult to maintain with the proliferation of ICTs enabling individuals to carry out typically 'private' activities in 'public' spaces. For example, one can communicate with friends, browse financial records, or even monitor one's heart rate on a public street via their smartphone. As concluded in Chapter 3, like a hermit crab individuals now carry their homes around with them - although in their pockets instead of on their backs.[998]

Despite these developments, the IP Act provides significantly less protection to individuals' metaphorical 'home 2.0' (and the data that flows from it) than to their non-digital, realspace lives.[999] This thesis has argued that the IP Act misconstrues the transferral of life online as an apathy towards privacy which has led to an insufficient system of protection for privacy in the digital age. It is, therefore, necessary for the law to recognise and amend its approach in line with the prevailing technocultural reality of the contemporary surveillance landscape.

This thesis subsequently argues that privacy needs to be re-conceptualised in more dynamic, non-spatial and non-physical terms in order for it to be preserved in the digital age - where physical boundaries no longer hold the same 'normative thrust' as they once did in the analogue era.[1000] This argument is supported by Nissenbaum's

---

[997] As argued in Chapter 4, Part 2, section 1.1.3.
[998] See Chapter 3, Conclusion.
[999] 'Home 2.0' taken from Koops (n 478).
[1000] Koops (n 478) 10.

'contextual integrity framework' which forms the basis of the following recommendation for re-conceptualising privacy in the digital age.

3.1.2.1 Privacy as a contextual value

Nissenbaum's 'contextual integrity framework' positions privacy as a contextual value that is to be protected by ensuring that personal information flows 'appropriately.'[1001] 'Appropriateness' is defined according to the social norms and rules governing the flow of information in distinct social contexts.[1002]

The 'contextual integrity framework' is intended for use as a benchmark for privacy and is structured according to 'context-relative information norms' which refer to the different practices and activities in different contexts.[1003] 'Context-relative information norms' are characterised by the following 'parameters:' contexts (eg education, work, health); actors (eg employee, friend, doctor); attributes/information types (eg healthcare information, relationship information, or financial information), and; transmission principles which refers to the constraints on the flow of information (eg confidentiality so the recipient cannot share the information).[1004] Should either of these components be changed by a practice (eg by the sharing of information to more actors than existed in the original context within which it was shared) that practice may be viewed as having violated entrenched informational norms and, in turn, contextual integrity. For example, in relation to the 'Cambridge Analytica' scandal; the 'contextual integrity' of 87 million Facebook users were violated because the actors and context of the data were altered upon its removal from the Facebook dwelling.[1005] Nissenbaum's framework thus determines privacy violations on the basis of transgressions from widely accepted expectations (as derived from the practices) of those in the relevant community.

[1001] Nissenbaum *Privacy in context* (n 22) 3.
[1002] Ibid.
[1003] Ibid, 140.
[1004] Ibid, 140-147.
[1005] Cambridge Analytica discussed in Chapter 3, Part 2, section 1.1.

Nissenbaum still uses boundaries but does so in a more nuanced way by employing a multiplicity of contexts rather than the overly simplistic public-private dichotomy which she considers

> 'a cruder version of contextual integrity, postulating only two contexts with distinct sets of informational norms for each – privacy constraints in private, anything goes in public.'[1006]

In terms of how the contextual integrity framework might actually be applied in the legal sphere, Nissenbaum calls for the courts to use it as a basis for determining the reasonableness of an expectation of privacy.[1007] Specifically, she advises that the judiciary do this by determining whether a practice is analogous enough to previous practices that society has deemed a violation of privacy.[1008] Although, there will arguably be limits to this approach where analogising or re-applying expectations from earlier practices will be too much of a stretch.[1009]

The contextual integrity framework can be seen, at least to some extent, under the GDPR where a strengthened right to erasure (or 'right to be forgotten') protects against the inappropriate flow of historic information into new contexts – regardless of whether or not that information was actively shared by the individual in 'public.'[1010] Accordingly, expectations of privacy are not dependent upon whether the information has been shared in 'public' or 'private,' but rather, on a change in context - a change in a component of the contextual integrity framework. This provides a good example of how the law might better conceptualise privacy - not as a spatially dependent right but as 'a right to live in a world in which our expectations about the flow of personal

---

[1006] Nissenbaum (n 22) 141.
[1007] Ibid, 233-234.
[1008] Ibid.
[1009] Bankston and Soltani propose the adoption of a 'cost-based analysis' by the courts to help evaluate expectations of privacy in relation to new surveillance practices. Whilst this a fairly abstract theory, it demonstrates an attempt to create a tool for the courts to evaluate expectations of privacy against new surveillance technologies. See, Kevin Bankston and Ashkan Soltani, 'Tiny constables and the cost of surveillance: making cents out of *United States v Jones*' (2014) 123 The Yale Law Journal 335.
[1010] GDPR (n 645), art 17.

information are, for the most part, met.'[1011] In doing so, the schism between experience and expectation created by digital technologies and practices is capable of being contested and challenged as a violation of privacy.[1012] Furthermore, via an 'expectation model,' privacy is better placed to move with the times and is less likely to become obsolete. In this sense, a more dynamic protection can be afforded to privacy that is consistent with the expectations of the community, and thus, works towards Murray's call for a more dynamic and symbiotic approach to regulating for cyberspace.

Whilst Nissenbaum's framework is widely considered a worthwhile contribution to the privacy debate, Brincker criticises it for falling short of providing an actual solution.[1013] She argues that Nissenbaum fails to take into consideration the agency of the people and things that actually make up a certain context.[1014] She further argues that Nissenbaum's definition of 'contextual integrity' adheres to prevailing norms and expectations instead of the functional value of a given context.[1015] Consequently, there is a risk of dysfunctional expectations forming the basis of privacy protections.[1016] For example, in a social networking context it might be expected that Facebook will gather and share data with other providers or state actors and, therefore, no privacy breach will occur.

Brincker subsequently argues that privacy should be regarded as relational and not just contextual, with privacy hinging on persons' ability to limit the social consequences of their actions; to be able to 'conceal *during* exposure.'[1017] Therefore, relational privacy centres around the ability to anticipate and create specific consequences; to avoid conditions of 'uncertainty and undue coercion.'[1018] Under this approach, harm occurs when surveillance is unpredictable and unknowable as it undermines the

---

[1011] Nissenbaum (n 22), 231.
[1012] Ibid
[1013] Maria Brincker, 'Privacy in public and the contextual conditions of agency' in Tjerk Timan, Bryce Clayton Newell, Bert-Jaap Koops, *Privacy in public: conceptual and regulatory changes* (Edward Elgar, 2017) 65.
[1014] Ibid.
[1015] Ibid 68.
[1016] Ibid.
[1017] As explained in Tjerk Timan, Bryce Clayton Newell, Bert-Jaap Koops, 'Introduction: conceptual directions for privacy in public space,' in Timan et al (n 1013) 4.
[1018] Brincker (n 1013) 89.

individuals' ability to control the consequences of their exposure. Accordingly, unregulated and unpredictable surveillance (such as the sharing of data by Facebook), would be considered harmful on the basis that it limits the individual's ability to control their exposure.[1019]

Reidenberg raises similar concerns over the viability of an approach that relies wholly on 'reasonable expectations' on the basis that in many contexts of the digital age we hold no 'reasonable' expectations of privacy.[1020] He argues that

> '[i]n the face of "ambient surveillance," how can any notion of a reasonable expectation of privacy survive? Even the notion that a boundary can be drawn around whether technology to assist discovering information is in general use or not in general use becomes irrelevant. Alternate data sources abound.'[1021]

He subsequently concludes that models based on 'reasonable expectations' fail to protect us against what he calls 'non-breach breaches of privacy' - where information is already in some way public.[1022] Reidenberg subsequently proposes that a 'true public sphere' that is 'governance-related' be distinguished from 'private-regarding' acts and facts with protection being developed for the latter.[1023] However, this thesis does not endorse this proposal on the basis that he returns to a public-private dichotomy, albeit a reiterated version, that fails to take into account the merging of the two realms. He also provides little guidance as to how and by whom these 'true public' and 'true private' spheres are to be distinguished and judged.[1024]

Therefore, this thesis concludes that a re-conceptualisation of privacy as a more versatile and dynamic value is needed in order for it to be enjoyed outwith the spatial remits of traditional notions of privacy. Despite Brincker and Reidenberg's criticism

---

[1019] Ibid 90.
[1020] Joel Reidenberg, 'Privacy in public' (2014) 69 University of Miami Law Review 141.
[1021] Ibid, 146-147.
[1022] Ibid, 149.
[1023] Ibid.
[1024] As also concluded by Brincker (n 1013) 70.

of the 'contextual integrity framework,' Nissenbaum moves towards a conception of privacy that is reflective of the diverse contexts of the digital age and the need to formulate privacy needs accordingly (as opposed to determining harm on the basis of a static, spatial notion of privacy). Nissenbaum shows that whilst boundaries can still be used by the law to demarcate what practices one can expect in different settings, they must reflect the landscape they are intended for in order to provide meaningful guidance of human behaviour and to exert a pull towards compliance.[1025] This supports the argument of this thesis that the law needs to attune to the technocultural realities of the contemporary surveillance landscape in order to provide adequate protection to privacy. However, in agreement with Brincker, development of Nissenbaum's theory is required in order for it to become a workable and enforceable legal concept. In particular, it must be considered how 'reasonable expectations' are to be formulated so that the 'dysfunctional expectations' warned of by Brincker, do not form the basis of privacy protections.

3.2 Re-positioning participation

The IP Act's response to the participation of the individual was described in terms of haystacks and needles in Chapter 4, with 'hays' of data being collected 'in case of' a 'needle' hiding amongst innocent communications.[1026] The impact of this approach on privacy was demonstrated via an analysis of BCD and BPD powers under Article 8 ECHR in Chapter 5.[1027] It was argued that if a more substantive approach to proportionality was taken by the ECtHR (as seen in *S and Marper v UK*),[1028] under which the negative consequences of the powers could be truly considered by the Court, a successful challenge could be made on the grounds of proportionality.[1029] However, it was concluded that in light of the ECtHR's typically procedural approach to proportionality in surveillance cases, scope exists for these powers to fulfil the necessity requirement under Article 8(2).[1030] In which case, the ECHR would fail to

[1025] Franck (n 65).
[1026] See further Chapter 4, Part 2, section 2.2.2.
[1027] See Chapter 5, Part 2, section 1.
[1028] *S and Marper v UK* (n 235).
[1029] See Chapter 5, Part 2, section 1.3.
[1030] See Chapter 5, Part 2, section 1.5.

correct the positioning of participation under the IP Act. Following an examination of the CJEU's approach in *Tele2/Watson*, it was argued that the ECtHR ought to evolve its approach to assessing the proportionality of surveillance practices by reconsidering its focus on the sensitivity of material when determining discretion.[1031] It was argued that this would provide a more adequate degree of protection to privacy in the digital age where information *about* a communication is increasingly more revelatory than what lies within.

In light of the above conclusions, this thesis resists the invocation of bulk powers in the IP Act on the basis that they pose a disproportionate interference with privacy (despite the potential for a different conclusion being reached by the ECtHR). It recommends their removal from the IP Act, leaving only the targeted versions of each power in operation; which remain in themselves fairly bulky due to their thematic nature.[1032] This conclusion is supported by the CJEU's judgment in *DRI* and *Tele2/Watson* where it held that bulk data retention was disproportionate and ought to be subject to restrictions, such as being used only for the investigation of serious crime or terrorism and be strictly necessary in pursuing these objectives.[1033]

By following the CJEU's lead, the participatory characteristic of the third wave landscape would be better positioned under the IP Act so that it is no longer manipulated into facilitating an unjustified extension of the state's surveillance reach. As it stands, the IP Act undermines the benefits of the democratisation of surveillance brought about by the digital age - a democratisation that enables the individual to watch the watcher, to challenge the elite, to develop intimate relationships, and to cultivate a better sense of self. The law must, therefore, protect the positive elements of surveillance washed in by the third wave and encourage the use of surveillance as a tool of democracy and resilience that can benefit the individual as opposed to just manipulate, coerce, and constrain. Thus, it is about respecting the different spheres of surveillance so much as it is about respecting spheres of privacy.

[1031] See Chapter 5, Part 2, section 1.4.
[1032] As shown in Chapter 4, Part 2, section 1.3.
[1033] See further Chapter 5, section 1.4.

3.3 Recognising the group

This thesis has argued that with increased data exhaust and advances in technological processing in the digital age, interferences with privacy increasingly take place on a group level; impacting societal as well as individual interests in privacy. However, due to the highly individualistic focus of Article 8, limited scope exists for the vindication of such a group right to privacy.[1034] The danger of this limited scope for privacy to be challenged on a non-individual basis was demonstrated in Chapter 4 via an examination of the harm caused by BCD and BPD powers under the IP Act.[1035] In agreement with Sloot, it was argued that mass data-focussed surveillance created a 'power relationship' that risked the arbitrary use of power and had Panoptic-type effects on both the individual and society.[1036] It was concluded that Article 8 must, therefore, be developed in response to the widening of the surveillance net so that this 'power relationship' can be challenged.

In terms of how this might be achieved, privacy scholars increasingly look to the 'non-domination' principle embraced by republicanism for use in cases concerning mass data-driven surveillance, as opposed to the 'non-interference' principle currently implemented by the ECtHR.[1037] Under the 'non-interference' principle, harm is caused when society interferes with individual choices that have no (harmful) effect on others.[1038] Thus, a person's freedom can only be justifiably interfered with when that freedom is used to interfere with the enjoyment of another's freedom. Freedom as 'non-interference' is thus equal to freedom from interference by third parties.[1039] Emphasis is thus placed on actual interferences occurring in order for freedom to be interfered with.

[1034] See Chapter 2, section 4.
[1035] Chapter 4, Part 2, section 3.
[1036] Ibid.
[1037] See Sloot (n 758); Bryce Newell, 'Technopolicing, surveillance, and citizen oversight: a neorepublican theory of liberty and information control' (2014) 31 Government Information Quarterly 421; Andrew Roberts, 'A republican account of the value of privacy' (2015) 14 European Journal of Political Theory 320.
[1038] Sloot, ibid, 545-546.
[1039] The non-interference principle is derived from John Stuart Mill, *On liberty and other writings* (Cambridge University Press, 1989); Sloot (n 758) 546.

The 'non-domination' principle, on the other hand, is less focussed on actual interferences and is more concerned with the *potential* for interference arising from a lack of safeguards against arbitrary use of power.[1040] Freedom as 'non-domination' is about eliminating risks of arbitrary interference and domination, enabling the individual to self-govern.[1041] Therefore, when determining an interference under the non-domination principle 'the core question shifts from the actual use of power to the potential to use the power.'[1042] Accordingly, if the ECtHR were to adopt a non-domination approach to determining privacy violations by the state, the applicant would not have to substantiate his or her claim of a concrete, personal harm caused by a particular surveillance practice. Rather, he or she would merely have to demonstrate that the government possesses the ability to use its power arbitrarily due to a lack of adequate safeguards.

In recent years, the ECtHR has shown more of a willingness to assess *in abstracto* claims in surveillance cases, particularly in the aforementioned cases of *Zakharov v Russia* and *Szabo and Vissy v Hungary*.[1043] The approach taken by the ECtHR in each of these cases is emblematic of the non-domination principle. In *Zakharov*, it set down conditions for an *in abstracto* claim to be made against surveillance legislation as follows: (i) the applicant can demonstrate that they are possibly affected by the surveillance, either because they belong to a group of persons targeted by the legislation or because the legislation directly affects all users of communication services by creating a system where any communication might be intercepted; (ii) there is a lack of effective remedies causing widespread suspicion and concern among the general public that secret surveillance measures are being abused.[1044] In such circumstances, the Court held that

---

[1040] Major work on 'non-domination' is Philip Pettit's *Republicanism: a theory of freedom and government* (Clarendon Press, 1997).
[1041] Bryce Newell, 'The massive metadata machine: liberty, power, and secret mass surveillance in the US and Europe' (2014) 10 A Journal of Law and Policy for the Information Society 481, 514-15.
[1042] Sloot (n 758) 546.
[1043] *Zakharov v Russia* (n 204); *Szabo and Vissy v Hungary* (n 266).
[1044] *Zakharov v Russia*, ibid, para 171.

> '[t]he menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8.'[1045]

It subsequently went on to assess the quality of the concerned legislation, thus emphasising the Court's interpretation of freedom as freedom from potential use of arbitrary power.[1046] Sloot argues that by shifting away from the 'non-interference' principle and victim requirement so explicitly in *Zakharov*, the ECtHR expanded the scope of Article 8 to allow for cases brought by legal persons and cases revolving around societal interests.[1047] In doing so, the 'power relationship' emerging from bulk, data-driven surveillance regimes (like the BCD and BPD powers under the IP Act) can be challenged and power can once again become verifiable.[1048]

Whilst the 'mere existence' test was previously used in *Klass v Germany*, the Court in *Zakharov* went further in terms of its explicit recognition of groups affected by states' propensity for mass surveillance of communications in the digital age.[1049] *Klass* might, therefore, be viewed as the foundation for the Court's approach in *Zakharov* which is more explicit in its abandonment of the requirement of actual and concrete harm and acceptance of group privacy claims.

Whilst this thesis advocates the adoption of the non-domination principle in cases concerning mass surveillance where it is difficult for the individual to substantiate personal harm, the ECtHR's acceptance of *in abstracto* claims poses some issues. For example, Sloot notes that the ECtHR's role as a Court of Fourth Instance is brought into question as not all domestic remedies need to be exhausted in order to bring a claim.[1050] Consequently, in these cases, the ECtHR would become a Court of First Instance which: (i) is not a power granted to it by the Convention; and, (ii) threatens

---

[1045] Ibid.
[1046] Ibid, para 302.
[1047] Sloot (n 758) 544.
[1048] For discussion of 'power relationship' see Chapter 4, Part 2, section 3.
[1049] *Klass v Germany* (n 199). For discussion of *Klass* and 'mere existence' test see Chapter 2, section 1.1.2.
[1050] Sloot (n 758) 548.

to 'undermine the position of national democratic orders.'[1051] The impact of these consequences needs to be explored fully before the ECtHR goes any further in its adoption of the non-domination principle and clear limits need to be placed on its acceptance of *in abstracto* claims. This being said, the republican approach offers a promising solution for the protection of privacy in the Big Data era where unknowable surveillance and non-personal harm flourishes.

However, in line with Murray's call for a hybrid regulatory model, it is held here that whilst the development of the ECtHR's approach takes a step towards enhancing the protection of (group) privacy in the digital age, this alone will not solve the societal issues posed by Big Data processes. This will also require a fundamental change of how data and privacy are perceived by institutional actors – as an expression of life within digital society that is worthy of protection rather than as detritus left over from apathetic individuals showcasing their lives online. Although recommendations for political and non-legal solutions are outwith the remit of this thesis, re-conceptualising privacy in terms of a contextual value as advocated by Nissenbaum (above), will help to encourage the development of such an approach by making privacy enforceable outwith the traditional spheres of privacy and determinable instead on the appropriateness of personal information flows.

4 Scope for future research

Due to the vastness of the surveillance landscape, there are various dimensions that could not be investigated within the remit of this thesis. Therefore, there are some areas in which future research could be carried out.

First, the focus of this research has been on the approach of UK surveillance law to the contemporary surveillance landscape. Comparative analysis could be carried out between the UK with other jurisdictions to determine how the UK's approach compares to that of other Western liberal democracies.

[1051] Ibid.

Second, as Brexit has not yet taken effect it is unclear how far the GDPR will be incorporated into UK data protection law. Whilst the Data Protection Act 2018 ('DPA 2018') provides important reform of data rights and imposes more obligations on industry, it includes a number of restrictions that leave it open to future challenge and potentially jeopardise the free flow of data with the EU once Brexit takes effect. In particular, the DPA 2018 includes broad exemptions from data rights and principles for: immigration control; the right not to be subjected to automated decision-making; special categories of data; cross-border transfer of data; national security certificates; intelligence services, and; freedom of expression purposes.[1052] There are also delegated powers that allow Ministers to add to these exemptions, meaning that individuals' data rights can be interfered with without parliamentary scrutiny.[1053] How these powers play out in the post-Brexit landscape will, therefore, impact the UK surveillance legal landscape.

There are also certain limitations of this thesis that would benefit from subsequent research. For example, it was argued that the haystack-needle approach in the UK has been *facilitated* by the transferral of life online and participation of the individual. It might also be useful to consider the extent to which the individual's participation online has *incentivised* the UK's aggressive approach to surveillance. Identifying the incentives behind the UK's approach would subsequently enable the reasons behind the IP Act to be critiqued, challenged, and corrected and used to develop a more effective and rights respecting culture of surveillance in the UK.

Furthermore, it was concluded above that Nissenbaum's contextual integrity framework represented a potential way forward in terms of how the law conceptualises privacy. However, it was held that this theory requires development in order to become an enforceable legal concept. Further research is thus needed here, although not only by legal scholars and philosophers. Other disciplines that engage with experiences of surveillance and privacy within the digital era should also be consulted, such as

---

[1052] DPA 2018, schedule 2.
[1053] Ibid, s 16. For criticism of delegated powers see: Delegated Power and Regulatory Reform Committee, *Sixth report of session 2017-19* (2017-19, HL 29); House of Lords Constitution Committee, *Data Protection Bill* (2017-19, HL 31), para 11.

different branches of geography and media studies. Given the extent to which technology now impacts expectations of privacy in different contexts by determining what is or is not possible, technologists should also be involved in the development of the contextual integrity framework as a foundation for surveillance law.[1054]

5 Thesis summary

This thesis has argued that UK law regulating state surveillance does not adequately protect privacy in the digital age because it fails to properly recognise the technological and cultural changes that the contemporary surveillance landscape has undergone. The importance of this research is placed on the value of privacy outlined in the Introduction to this thesis.

Chapter 1 conducted an historical survey of surveillance which illustrated the surveillance landscape prior to its digitalisation in the 21st century. It also served a definitional purpose with surveillance being distinguished from pure information gathering practices. The chapter was approached thematically via the themes of: tax and social welfare; crime and disorder; war; and, national security. These themes illustrated the varying uses of surveillance and the peaks and troughs of its use across different contexts. It was concluded that surveillance was a practice related to, but separate from, information gathering and that it begins when information is gathered 'in case of' instead of being absolutely necessary for achieving a specific aim or purpose. It was also concluded that the legal coverage of surveillance took some time to develop in the UK and, as shown by the Snowden disclosures, this legislative lag has persisted into the 21st century.

Having established the definition of surveillance in Chapter 1, Chapter 2 explored the definition of privacy under Article 8 ECHR. This was achieved via an examination of its application by the ECtHR in its surveillance case law. This chapter provided a benchmark against which the IP Act was subsequently assessed in Chapter 5. Chapter 2 adopted the structure of the ECtHR's assessment of interferences with Article 8 as

[1054] In a Goffmanian sense, technology sets the stage of possible action. See Erving Goffman, *Behaviour in public places* (The Free Press, 1966).

follows: (i) engaging Article 8(1); (ii) the legality of interferences, and; (iii) justified interferences. In relation to the triggering of Article 8(1), it was shown that only interception, and technically similar practices, were capable of engaging the right at the initial gathering stage of surveillance. Otherwise, it took the processing (and potential for processing) or retention of information to trigger the right.

Chapter 2 also considered the potential scope for group privacy under Article 8 in light of the ECtHR's expansion of the notion of victimhood in *Klass* where it allowed a challenge against the 'mere existence' of legislation permitting interception, meaning that actual personal harm did not have to occur in order for Article 8 to be engaged. It was concluded that whilst this represented an acknowledgment by the ECtHR of the inherently secret nature of surveillance and the resulting difficulties in substantiating an interference, 'groups' in the true sense were unable to claim an Article 8 right.

Chapter 2 concluded that the ECtHR has typically adopted broad notions of private life, harm, victimhood, and expectations of privacy in its surveillance case law. The importance of this was highlighted in relation to the contemporary surveillance landscape where the digitalisation of society has created new types of information and opportunities for surveillance that challenge traditional concepts of privacy (such as the existence of privacy in public space). However, the ECtHR's emphasis on the gradations of an intrusion, or layering of information, when assessing the necessity and proportionality of an interference was critiqued for unduly limiting the protection of Article 8 in the digital age where mass surveillance practices are increasingly directed toward the gathering of communication data which may not be sensitive enough to trigger the Court's application of stricter safeguard principles or to restrict the margin of appreciation awarded to states.

Chapter 3 then engaged in a theoretical discussion of the contemporary surveillance landscape to illustrate developments in surveillance brought about by technocultural change. It adopted the structure of 'waves' which was inspired by Galic et al's work

on the phases of surveillance theory.[1055] First wave theories included Bentham's Panopticon and Foucault's panopticism. First wave surveillance was shown to be: architectural; disciplinary; hierarchical; and geared towards the internalisation of the whips. The second wave referred to post-panoptical theories and the main theory examined here was Haggerty and Ericson's 'surveillant assemblage.'[1056] Haggerty and Ericson sought to tear down the walls of the panopticon, viewing it as an outdated conceptualisation of surveillance within the consumer capitalist society where surveillance was taken over by corporations and directed towards persons' data as opposed to their physical beings in order to control rather than discipline. Finally, third wave theories represented the contemporary surveillance landscape and emphasised the diversity in actors and purposes of surveillance brought about by the digitalisation and democratisation of surveillance.

Unlike the other waves, the third wave did not represent a shift away from or revision of first and second wave surveillance theories, but rather, an expansion or development of them that demonstrated the hybridity of the contemporary surveillance landscape. This was illustrated via an overview of three branches of the third wave: alternative opticons; sousveillance; participatory surveillance. The reality of the third wave was then illustrated by an examination of social media and smartphones which were used as 'sites of third wave surveillance.' These sites demonstrated the vertical and non-vertical axes of surveillance at play in the contemporary landscape and the interaction between them. The author's own theory of 'autobiographical surveillance' was also developed here as means of conceptualising digital data exchanges on social media as a form of participatory surveillance. This theory underlined the benefits bestowed on civil society by the democratisation of surveillance and demonstrated that expectations of privacy can exist within such realms of exposure. Three legal implications of the third wave were identified in this chapter: collapsing dichotomies; positioning participation; and, group privacy.

[1055] Galic et al, Bentham, Deleuze and beyond' (n 65); Galic et al, 'Surveillance theory and its implications for law' (n 64).
[1056] Haggerty and Ericson (n 362).

Chapter 4 established the UK's approach to the contemporary surveillance landscape via an analysis of the IP Act's response to the legal implications of the third wave identified in Chapter 3. It was established that the IP Act failed to adapt to the collapse of dichotomies, maintaining outdated distinctions that posed a threat to the protection of privacy. It was also concluded that the IP Act failed to properly position the participation of the individual by adopting a haystack-needle approach to surveillance. Instead of appreciating that the individual is now an actor of surveillance, who often exposes themselves as part of reciprocal relationships of watching, the IP Act misconstrues participation in digital data exchanges to facilitate an expansion of state surveillance. This has resulted in an unjustified extension of the state's surveillance reach and undermines the benefits bestowed on civil society by the third wave. Finally, it was argued that the bulk, data-focussed powers underlined the need for a group privacy right to be developed under Article 8 ECHR as these powers made it difficult for individuals to substantiate concrete and personal harm and, therefore, to challenge the 'power relationship' emerging from these practices.

Chapter 5 assessed the impact of the UK's approach to the contemporary surveillance landscape on the protection of privacy by analysing the IP Act under Article 8 ECHR. First, the haystack-needle approach was examined via an assessment of the BCD and BPD powers. It was concluded that the proportionality of these powers was questionable and that this resulted from the law's failure to appreciate the participation of the individual and, subsequently, her expectations of privacy in the digital age. However, due to the ECtHR's preference for a more pragmatic proportionality assessment, it was shown that scope existed for these powers to be deemed lawful. It was thus concluded that the ECtHR had to develop its determination of discretion and carry out more intensive scrutiny of surveillance in order to correct the positioning of participation under the IP Act and preserve privacy in the digital age. Second, the IP Act's response to the collapse of dichotomies was assessed via an analysis of the impact of the content-data distinction on safeguards applied to content and data-focussed powers. Weaker safeguards were shown to apply to data-focussed powers whereas stronger safeguards applied to interception and EI powers. In light of dangers posed by data-focussed powers, it was concluded that the weaker safeguards provided inadequate protection to privacy. However, it was shown that the ECtHR also

maintained this distinction between content and data, applying only general safeguard principles to data-focussed powers. It was subsequently concluded that the ECtHR needs to re-consider its determination of applicable safeguards in order to acknowledge the harm emanating from data-based surveillance.

Finally, this thesis has concluded with recommendations aimed at enhancing the IP Act's protection of privacy in the digital age. This thesis has argued that the Act needs to attune to the technocultural realities of the contemporary surveillance landscape and so recommendations were aimed at: (i) re-positioning participation; (ii) re-constructing boundaries; and, (iii) recognising the group. It is argued that these legal modifications will also protect the benefits that the contemporary surveillance landscape has bestowed on civil society, enabling individuals to participate in surveillance culture without forsaking their expectations of privacy.

6 Concluding remarks

In 1906, John Philip Sousa, an American composer and conductor, wrote an essay called 'The Menace of Mechanical Music,' in which he expressed grave concerns about the gramophone.[1057] He refers to the gramophone as a 'talking machine' and argues that it will destroy artistic expression by reducing people to passive listeners and suffocating individuals' own production of music.[1058] Sousa feared that the gramophone would suppress the individual's ability to participate in the development of their culture by confining creativity to the owners of the technology.

Lessig argues that Sousa's fears were well-founded, with culture becoming heavily professionalised and individuals being left with very little room to participate; thereby reducing culture to 'read-only.'[1059] However, he argues that a 'read-write' culture has been revived by the internet which enables individuals to once again contribute to society in a variety of different creative ways and to communicate their message to

[1057] John Philip Sousa, 'The menace of mechanical music' (1906) 8 *Appleton's Magazine* 278.
[1058] Sousa, ibid, 283.
[1059] Lawrence Lessig, 'Laws that choke creativity' (*TED talk*, 15 November 2007) <https://www.youtube.com/watch?v=7Q25-S7jzgs> accessed 18 March 2018.

large audiences.[1060] Lessig uses this to argue that copyright laws need to recognise the return of the read-write culture and not punish individuals for taking and re-editing copyrighted clips and tracks online to produce new types of content.[1061] Whilst copyright laws are not at issue in this thesis, the sentiment of Lessig's argument can be applied more generally to the context of the contemporary surveillance landscape in arguing that the law needs to protect and respect individuals as actors of surveillance instead of reducing them to passive objects of surveillance only capable of being controlled and disciplined by the elite.

The power of the individual to surveil was demonstrated through an examination of social media and smartphones as sites of third wave surveillance in Chapter 3. These examples showed that surveillance has now become an integral aspect of individuals' engagement with one another and, indeed, themselves. In addition, with this democratisation of surveillance, individuals have become able to scrutinise the elite who no longer sit hidden from view in a watchtower above them. In this sense, surveillance has enabled the individual to participate more actively and meaningfully in society on both a personal and political level. No longer need the individual sit as a passive object in a 'watch-only' 'surveillance state,' but rather, as an active participant in a community of dots capable of establishing and overturning surveillance norms and regulations within a 'surveillance culture.'

However, this thesis has shown that the value of surveillance as a tool for democracy is under threat from UK surveillance law. Instead of evolving to reflect the undulations of the third wave landscape and harness the democratic benefit from diversified surveillance ownership, the IP Act denies the role of human agency in the surveillance landscape and represents a clawing back of the hierarchical structure of surveillance characteristic of Bentham's prison-Panopticon. The importance of correcting laws so that they are reflective of the surveillance reality thus lies in the fact that it is not only

[1060] Ibid.
[1061] Ibid.

the right to privacy at stake, but so too a right to watch as a way of life – a right to surveillance.

References

Books

Alford S, *The Watchers: A Secret History of the Reign of Elizabeth I* (Bloomsbury Press, 2012)

Andrew C, *The Defence of the Realm: the authorised history of MI5* (Penguin, 2010)

Ang I and Symonds M (eds) *Home, displacement, belonging, communal/plural 5* (NSW Research Centre in Intercommunal Studies, 1997)

Avegerou C, Mansell R, Quah D, Silverstone R (eds) *The Oxford handbook of information and communication technologies* (Oxford University Press, 2009)

Barak A, *Proportionality: Constitutional rights and their limitations* (Cambridge University Press, 2012)

Barney D, Coleman G, Ross C, Sterne J, Tembeck T (eds), *The participatory condition* (University of Minnesota Press, 2015)

Basch L, Schiller N, Blanc C, *Nations unbound: transnational projects, postcolonial predicaments and deterritorialized nation-states* (Routledge, 1994)

Ball K and Webster F, *The intensification of surveillance: crime, terrorism and warfare in the information age* (Pluto Press, 2003)

Bennett C and Raab C, *The governance of privacy: policy instruments in global perspective* (MIT Press, 2006)

Bentham J, *The Panopticon writings (Ed. Miran Boovic)* (Radical Thinkers, 2010)

Bernal P, *Internet privacy rights: rights to protect autonomy* (Cambridge University Press, 2014)

Brownsword R and Yeung K (eds) *Regulation technologies: legal futures, regulatory frames and technological fixes* (Hart publishing, 2008)

Brownsword R and Yeung K (eds), *Routledge handbook of the law and regulation of technology* (Edward Elgar Publishing, 2017)

Caplan J and Torpey J (eds) *Documenting Individual Identity: The Development of State Practices in the Modern World* (Princeton University Press, 2001)

Cass Sunstein, *Republic.com 2.0* (Princeton University Press, 2009)

Colquhoun P, *A treatise on indigence* (Mawman, 1806)

Colquhoun P, *A treatise on the police of the Metropolis* (Mawman, 1800)

Dandekar C, *Surveillance, Power and Modernity. Bureaucracy and Discipline from 1700 to the Present Day* (Polity Press, 1990)

Davis F, McGarrity N, Williams G (eds.) *Surveillance, counter-terrorism and comparative constitutionalism* (Taylor & Francis, 2014)

de Certeau M, *The practice of everyday life* (1988, University of California Press).

Dean M, *Governmentality: power and rule in modern society* (2nd edn, 2010, Sage publishing)

Deleuze G and Guattari F, *A Thousand Plateaus*: *capitalism and schizophrenia* (Minnesota Press, 1987)

Donohue L, *Counter-Terrorist Law: And Emergency Powers in the United Kingdom 1922-2000* (Irish Academic Press, 2001)

Etzioni A, *The limits of privacy* (Basic Books, 1999)

Foucault M, *Discipline and punish: the birth of the prison* (Penguin, 1991)

Foucault M, Martin L, Guttman H, Hutton P, *Technologies of the self* (University of Massachusetts Press, 1988)

Foucault M, *Power: volume 3* (Penguin, 2002)

Foucault M, *The birth of biopolitics: lectures at the College de France 1978-79* (Palgrave Macmillan, 2008)

Foucault M, *The history of sexuality volume I: an introduction* (Vintage Books, 1978).

Fraser D, *The Evolution of the British Welfare State* (2nd edn, Palgrave Macmillan, 1984)

Fredman J (ed) *The mobile story: narrative practices with locative technologies* (2013, Routledge)

Fuchs C (ed) *Internet and surveillance: challenges of Web 2.0* (Routledge, 2012)

Goffman E, *Behaviour in public places* (The Free Press, 1966)

Greer S, *The margin of appreciation: interception and discretion under the European Convention of Human Rights* (Council of Europe, 2000)

Gutwirth S, Leenes R, de Hert P, Poullet Y (eds) *European data protection: coming of age* (Springer, 2013).

Haigh C, *Elizabeth I* (Routledge, 2013)

Harvey S, *Domesday: Book of Judgment* (Oxford University Press, 2014)

Haynes A, *The Elizabethan Secret Service* (Kindle DX Version, The History Press, 2009)

Keeton G and Shwarzenberger G (eds) *Jeremy Bentham and the law: a symposium* (Steven & Sons ltd, 1948)

Latour B, *Reassembling the social: an introduction to actor-network-theory* (OUP, 2005)

Legg A, *The margin of appreciation in international human rights law* (Oxford, 2012)

Lennon G and Walker C (eds), *Routledge Handbook of Law and Terrorism* (Routledge, 2015)

Lessig L *Code and other laws of cyberspace* (Basic Books, 1999)

Lessig L, *Code version 2.0* (Basic Books, 2006)

Levi-Faur D (ed) *Handbook on the politics of regulation* (Edward Elgar, 2011)

Long D, *Bentham on Liberty: Jeremy Bentham's idea of liberty in relation to his utilitarianism* (University of Toronto Press, 1977)

Lustgarten L and Leigh I, *In from the cold: national security and parliamentary democracy* (Clarendon Press, 1994)

Lyon D and Bauman Z, *Liquid surveillance: a conversation* (Polity Press, 2013)

Lyon D *Theorizing surveillance: the panopticon and beyond* (Wilan Publishing, 2006)

Lyon D, *Surveillance after September 11* (Polity Press, 2003)

Lyon D, *Surveillance after Snowden* (Polity, 2014)

Lyon D, *Surveillance society: monitoring everyday life* (Open University Press, 2001)

Lyon D, *Surveillance studies: an overview* (Polity Press, 2007)

Lyon D, *The Culture of Surveillance* (Polity Press, 2018)

Macdonald R, Matxcher F and Petzold H (eds) *The European system for the protection of human rights* (Kluwer Academic Publishers, 1993)

MacKinnon C, *Toward a feminist theory of the state*, (Harvard University Press, 1989)

Malksoo L and Benedek W, *Russia and the European Court of Human Rights: the Strasbourg effect* (Cambridge University Press, 2017)

Malthus T, *An Essay on the Principle of Population, as it Affects the Future Improvement of Society with Remarks on the Speculations of Mr. Godwin, M.*

Condorcet, and Other Writers (First printed 1798, Electronic Scholarly Publishing Project, 1998)

Mayer-Schronberger V, *Delete: the virtue of forgetting in the digital age* (Princeton University Press, 2009)

McCaffrey W, *Elizabeth I* (Edward Arnold, 2001)

Mill JS, *On Liberty*, (Digireads.com, 2010)

Miller R (ed) *Privacy and power: a transatlantic dialogue in the shadow of the NSA affair* (Cambridge University Press, 2017)

Murray A, *Information technology law: the law and society* (3rd edn, Oxford University Press, 2016)

Neal A, *Security in a small nation* (Open Book Publishers, 2017)

Newton D, *North-East England, 1569-1625: Governance, Culture and Identity* (Boydell Press, 2006)

Newton Lee (ed) *Counterterrorism and cybersecurity* (2nd edn, Springer, 2015)

Nissenbaum H, *Privacy in context: technology, policy, and the integrity of social life*' (Stanford University Press, 2010)

Okin S M, *Justice, gender and the family* (Basic Books, 1989)

Olsson T (ed.) *Producing the Internet: critical perspectives of social media* (Nordicom, 2013)

Orwell G, *Nineteen Eighty-Four* (First published 1949, Penguin, 2013)

Pariser E, *The filter bubble: what the internet is hiding from you* (Penguin, 2012)

Pettit P, *Republicanism: a theory of freedom and government* (Clarendon Press, 1997)

Poster M, *The mode of information: poststructuralism and social context* (University of Chicago Press, 1990)

Raz J, *The Authority of Law* (Oxford, 1979)

Regan P, *Legislating for privacy: technology, social values, and public policy* (University of North Caroline Press, 1995)

Richards N, *Intellectual privacy: rethinking civil liberties in the digital age* (Oxford, 2015)

Richelson J, *A century of spies: intelligence in the Twentieth century* (Oxford University Press, 1995)

Rosen F, *Classical utilitarianism: from Hume to Mill* (Routledge, 2003)

Rosen F, *Jeremy Bentham and representative democracy: a study of the constitutional code* (Oxford Clarendon Press, 1983)

Rosen J, *The unwanted gaze: the destruction of privacy in America* (Vintage Books, 2000)

Rossler B, Mokrosinska D (eds) *Social dimensions of privacy: interdisciplinary perspectives* (Cambridge, 2015)

Rossler B, *The value of privacy* (Polity Press, 2005)

Ryan A (ed) *J.S. Mill and Jeremy Bentham: utilitarianism and other essays* (Penguin Books, 2004)

Schartum et al (eds) *Jon Bing: en hyllest/a tribute* (Gyledendal, 2014)

Schoeman F, *Philosophical dimensions of privacy: an anthology* (Cambridge University Press, 1984)

Schofield P, *Bentham: a guide for the perplexed* (Continuum, 2009)

Scholz T (ed.) *Digital Labour: the internet as playground and factory* (Routledge, 2013)

Slack P, *Poverty and Policy in Tudor and Stuart England* (Longman, 1988)

Solove D, *Understanding Privacy* (Harvard University Press, 2008)

Sottiaux S, *Terrorism and the limitation of rights: The ECHR and the US constitution* (Hart publishing, 2008)

Stafford D, *Churchill and the secret service* (Abacus, 2001)

Sunstein C, *Republic.com 2.0* (Princeton University Press, 2009)

Taylor L, Floridi L, van der Sloot B (eds) *Group Privacy: new challenges of data technologies* (Springer, 2017)

Thomas D and Loader B, *Cybercrime: law enforcement, security, and surveillance in the Information Age* (Routledge, 2000)

Thompson F (ed) *The Cambridge Social History of Britain 1750-1950, Volume 5: Social Agencies and Institutions* (Cambridge University Press, 1990)

Thompson J, *The media and modernity: a social theory of the media* (Stanford University Press, 1995)

Timan et al (eds) *Privacy in public space: conceptual and regulatory challenges* (Elgar Law, 2017)

Trottier D, *Social media as surveillance*: *rethinking visibility in a converging world* (Ashgate publishing, 2012)

Van Dijk, van Hoof, van Rijn, and Zwaak, *Theory and Practice of the European Convention on Human Rights* (4th edn, Intersentia, 2006)

Viadhyanathan S, *The Googlization of everything (and why we should worry)* (University of California Press, 2011)

Westin A, *Privacy and freedom* (Ig publishing, 2015)

Whitaker R, *The end of privacy: how total surveillance is becoming a reality* (The New Press, 1999)

Wilkinson and Stewart A (eds) *Contemporary Research on Terrorism* (Aberdeen University press, 1987)

Williams R, *Culture & Society: 1780-1950* (Chatto & Windus, 1958)

Wilson R and Adam I, *Special Branch a history 1883-2006* (Biteback publishing, 2015)

Wolfe W, *Winning the War of Words: Selling the War on Terror from Afghanistan to Iraq* (Praeger Publishers, CT 2008)

Journal Articles

Albrechtslund A and Dubbeld L, 'The plays and arts of surveillance: studying surveillance as entertainment' (2005) 3 Policy Studies 216

Albrechtslund A, 'Online social networking as participatory surveillance' (2008) 13(3) First Monday 1

Allen A and Mack E, 'How privacy got its gender' (1990) 10 Northern Illinois University Law Review 441

Andrejevic M, 'The big data divide' (2014) 8 International Journal of Communications 1673

Andrejevic M, 'The work of watching one another: lateral surveillance, risk, and governance' (2005) 2 Surveillance & Society 479

Bamford B, 'The Role and Effectiveness of Intelligence in Northern Ireland' (2006) 20 Intelligence and National Security 4

Bankston K and Soltani A, 'Tiny constables and the cost of surveillance: making cents out of *United States v Jones*' (2014) 123 The Yale Law Journal 335

Bennett C, Regulating privacy: data protection and public policy in Europe and the United States (Cornell University Press, 1992)

Benvenisti E, ‘Upholding democracy amid the challenges of new technology: what role for the law of global governance?’ (2018) 29 European Journal of International Law 9

Bernal P, ‘The right to be forgotten in the post-Snowden era’ (2014) 1 Privacy in Germany 1

Bevitt A and Dietschy L, ‘GDPR series: the risks with data profiling’ (2016) 17 Privacy & Data Protection 6

Black J, ‘Decentring regulation: understanding the role of regulation and self regulation in a ‘Post-Regulatory’ world’ (2001) 54 Current Legal Problems 103

Boone K, ‘Privacy and community’ (1983) 9 Theory and Social Practice 1

Boyd D and Ellison N, ‘Social network sites: definition, history, and scholarship’ (2007) 13 Computer-Mediated Communication 210

Camacho S, ‘Can you hear me now? Time to consider whether cell phone providers are state actors’ (2016) 49 Suffolk University Law Review 257

Chan C, ‘Proportionality and invariable baseline intensity of review’ (2013) Legal Studies 1

Clutterbuck L, ‘Countering Irish republican terrorism in Britain: its origin as a police function’ (2006) 18 Terrorism and Political Violence 95

Cohen J, ‘DRM and privacy’ (2003) 18 Berkeley Technology Law Journal 575

Cohen J, ‘Studying law studying surveillance’ (2015) 13 Surveillance & Society 91

Coleman S, ‘Email, terrorism, and the right to privacy’ (2006) 8 Ethics and Information Technology 17

de Souza e Silva A and Sutko D, ‘Playing life and living play: how hybrid reality games reframe space, play, and the ordinary’ (2008) 25 Critical Studies in Media Communication 447

Deleuze G, ‘Postscript on societies of control’ (1992) 59 October 3

Dholakia N and Zwick D, ‘Privacy and consumer agency in the information age: between prying profilers and preening webcams’ (2001) 1 Journal of Research for Consumers 1

Edwards L and Urquhart L, ‘Privacy in public spaces: what expectations of privacy so we have in social media intelligence?’ (2016) 24 International Journal of Law and Information Technology 279

Elliott M, ‘The HRA 1998 and the standard of substantive review’ (2002) 7 JR 97

Esen R, ‘Intercepting communications ‘in accordance with the law’ (2012) 76 Journal of Criminal Law 164

Franck T, ‘Legitimacy in the international system’ (1988) 82 American Journal of International Law 705

Frank F, ‘The expansion of intelligence agency mandates: British counter-terrorism in comparative perspective’ (2009) 35 Review of International Studies 983

Frantziou E, ‘Further developments in the right to be forgotten: the European Court of Justice’s judgement in the Case C-131/12, *Google Spain, SL, Google Inc v Agencia Espanola de Protection de Datos* (2014) 0 Human Rights Law Review 1

French M and Smith G, ‘“Health” surveillance: new modes of monitoring bodies, populations, and polities’ (2013) 23 Critical Public Health 383

Fuchs C, ‘Digital presumption labour on social media in the context of the capitalist regime’ (2014) 23 Time and Society 97

Fuchs C, ‘Surveillance and critical theory’ (2015) 3 Media and Communication 6

Galic et al, ‘Bentham, Deleuze and beyond: An overview of surveillance theories from the Panopticon to participation’ (2017) 30 Philosophy of Technology 9

Gandy O, ‘Consumer protection in cyberspace’ (2011) 2 Triple C 175

Garrido V, ‘Contesting a biopolitics of information and communications: the importance of truth and surveillance after Snowden’ (2015) 13 Surveillance & Society 153

Gavison R, ‘Feminism and the public-private distinction’ (1992) 45 Stanford Law Review 1

Gillespie A, ‘Regulation of internet surveillance’ (2009) 4 European Human Rights Law Review 552

Goldsmith J, ‘Against cyberanarchy’ (1998) 65 Chicago Law Review 1199

Goold B, ‘Surveillance and the political value of privacy’ (2009) 1 Amsterdam Law Forum 3

Granger M and Irion K, ‘The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection’ (2014) 39 European Law Review 835

Groening S, ‘From “a box in the theatre of the world” to “the world as your living room”: Cellular phones, television and mobile privatisation’ (2010) 12 New Media & Society 1331

Haggerty K and Ericson R, ‘The surveillant assemblage’ (2000) 51 The British Journal of Sociology 605

Hatuka T and Toch E, ‘Being visible in public space: the normalisation of asymmetrical visibility’ (2017) 54 Urban Studies 984

Hier S, ‘Probing the surveillant assemblage: on the dialectics of surveillance practices as processes of social control’ (2003) 3 Surveillance & Society 399

Johnson D and Post D, ‘Law and borders: the rise of law in cyberspace’ (1996) 48 Stanford Law Review 1367

Joinson A, ‘Looking at, ‘looking up’ or ‘keeping up with’ people? Motives and use of Facebook (2008) CHI-2008 Proceedings 1027

Koops B, ‘On legal boundaries, technologies, and collapsing dimensions of privacy’ (2014) 3 Politica e Societa 247

Koops B, ‘The trouble with European data protection law’ (2014) 4 International Data Privacy Law 250

Koskela H, ‘Webcams, TV shows, and mobile phones: empowering exhibitionism’ (2004) 2 Surveillance & Society 199

Lampe C, Ellison N, and Steinfield C, ‘A Face (book) in the crowd: Social searching vs. social browsing’ (2006) In proceedings of the 2006 20th anniversary conference on computer supported cooperative work 167

Larsson S, ‘A first line of defence? Vigilant surveillance, participatory policing, and the reporting of “suspicious” activity’ (2016) 15 Surveillance & Society 94

Lemely M, ‘Private property’ (2000) 52 Stanford Law Review 1545

Lennon G, ‘Precautionary tales: suspicionless counter-terrorism stop and search’ (2015) 15 Criminology and Criminal Justice 44

Lessig L, ‘The new Chicago School’ (1999) 27 Journal of Legal Studies 661

Lessig L, ‘The zones of cyberspace’ (1996) 48 Stanford Law Review 1403

Lupton D, ‘M-health and health promotion: the digital cyborg and surveillance society’ (2012) 10 Social Theory & Health 229

Lyon D, ‘Surveillance, Snowden, and big data: capacities, consequences, critique’ (2014) Big Data & Society 1.

Maguire K, ‘The Intelligence War in Northern Ireland’ (1988) 4 International Journal of Intelligence and Counterintelligence 2

Mann S, Nolan J, Wellman B, ‘Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments’ (2003) 1 Surveillance & Society 331

Marguiles P, ‘Surveillance by algorithm: the NSA, computerised intelligence collection, and human rights’ (2016) 68 Florida Law Review 1045

Marwick A, ‘The public domain: social surveillance in everyday life’ (2012) 9 Surveillance and Society 378

Mathieson T, ‘The viewer society: Michael Foucault’s “panopticon revisited”’ (1997) 1 Theoretical Criminology 215

McArthur R, ‘Reasonable expectations of privacy’ (2001) 3 Ethics and technology 123

McHarg A, ‘Reconciling human rights and the public interest: Conceptual problems and doctrinal uncertainty in the jurisprudence of the European Court of Human Rights’ (1999) 62 The Modern Law Review 671

McMullan J, ‘Social Surveillance and the rise of the “police machine”’ (1998) 2 Theoretical Criminology 93

McMullan J, ‘The arresting eye: discourse, surveillance and disciplinary administration in early English police thinking’ (1998) 7 Social and Legal Studies 97

Millinton B, ‘Smartphone apps and mobile privatisation of health and fitness’ (2014) 31 Critical Studies in Media Communication 479

Moran J, ‘Evaluating special branch and the use of informant intelligence in Northern Ireland’ (2010) 25 Intelligence and National Security 1

Moreham N, ‘The right to respect for private life in the European Convention on Human Rights: a re-examination’ (2008) 1 European Human Rights Law Review 44

Murphy M, ‘A shift in the approach of the European Court of Human Rights in surveillance cases: a rejuvenation of necessity?’ (2014) European Human Rights Law Review 507

Murphy M, ‘The relationship between the European Court of Human Rights and national legislative bodies: Considering the merits and risks of the approach of the Court in surveillance cases’ (2013) 3 Irish Journal of Legal Studies 65

Murray A and Scott C, ‘Controlling the new media: hybrid responses to new forms of power’ (2002) 65 MLR 491

Newell B, ‘Technopolicing, surveillance, and citizen oversight: a neorepublican theory of liberty and information control’ (2014) 31 Government Information Quarterly 421

Newell B, ‘The massive metadata machine: liberty, power, and secret mass surveillance in the US and Europe’ (2014) 10 A Journal of Law and Policy for the Information Society 481

Nissenbaum H, ‘Privacy as contextual integrity’ (2004) 79 Washington Law Review 119

O’Floinn M and Ormerod D, ‘Social networking sites, RIPA, and Criminal investigations’ (2011) 10 Criminal Law Review 766

O'Leary S, 'Balancing rights in a digital age' (2018) Irish Jurist 59

Olsen F, 'The family and the market: a study of ideology and legal reform' (1983) 96 Harvard Law Review 1497

Patton P, 'Metamorphologic: bodies and powers in a thousand plateaus' (1994) 25 Journal of the British Society for Phenomenology 157

Poster M, 'Consumption and digital commodities in the everyday' (2004) 18 Cultural Studies 409

Poudel S, 'Internet of things: underlying technologies, interoperability, and threats to privacy and security' (2016) 31 Berkeley Technology Law Journal 997

Reid R, 'The Rebellion of the Earls, 1569: The Alexander Prize 1905' (1906) 20 Transactions of the Royal Historical Society 171

Reidenberg J, 'Lex informatica: the formulation of information policy rules through technology' (1998) 76 Texas Law Review 1439

Reidenberg J, 'Privacy in public' (2014) 69 University of Miami Law Review 141

Rivers J, 'Proportionality and variable intensity of review' (2006) 65 The Cambridge Law Journal 174

Roberts A, 'A republican account of the value of privacy' (2015) 14 European Journal of Political Theory 320

Romele A, Gallino F, Emmenegger C, Gorgone D, 'Panopticism is not enough: social media as technologies of voluntary servitude' (2017) 15 Surveillance & Society 204

Rotenberg M, ‘Fair information practices and the architecture of privacy: (What Larry doesn’t get)’ (2001) 1 Stanford Law Review 89

Ruiz B, ‘Privacy in telecommunications: A European and an American Approach’ (The Hague: Kluwer Law International, 1996)

Scassa T, ‘Law enforcement in the age of big data and surveillance intermediaries: Transparency challenges’ (2017) 14 Scripted 2.

Schwartz P, ‘Beyond Lessig’s code for internet privacy: cyberspace filters, privacy control, and fair information practices’ (2000) Wisconsin Law Review 243

Schwartz P, ‘Privacy and democracy in cyberspace’ (1999) 52 Vanderbilt Law Review 1609

Semitsu J, ‘From Facebook to mug shot: how the death of social networking privacy rights revolutionised online government surveillance’ (2011) 31 Pace Law Review 1

Sharon T, ‘Self-tracking for health and the quantitative self: re-articulating autonomy, solidarity, and authenticity, in an age of personalised healthcare’ (2017) 30 Philosophy & Technology 93

Shilton K, ‘Four billion little brothers? Privacy, mobile phones, and ubiquitous data collection’ (2009) 52 Communications of the ACM 48

Solove D, ‘“I’ve got nothing to hide” and other misunderstandings of privacy’ (2008) 44 San Diego Law Review 745

Sousa J, ‘The menace of mechanical music’ (1906) 8 Appleton’s Magazine 278

Stuntz W, ‘Secret service: against privacy and transparency’ (2006) 234 New Republic 12

Tokunaga R, ‘Social networking site or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships’ (2011) 27 Computers in human behaviour 705

Tokunga R, ‘Social networking or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships’ (2011) 27 Computers in Human Behaviour 705

Tomkins A, ‘Intercepted Evidence: Now You Hear Me, Now You Don’t’ (1994) 57 Modern Law Review 941

Trottier D, ‘A research agenda for social media surveillance’ (2011) 8 Fast capitalism 1

Trottier D, ‘Interpersonal surveillance on social media’ (2012) 37 Canadian Journal of Communication 319

Trottier D, ‘Open source intelligence social media and law enforcement: visions, constraints and critiques’ (2015) 18 European Journal of Cultural Studies 530

Tsakyrakis S, ‘Proportionality: An assault on human rights?’ (2009) 7 International Journal of Constitutional Law 468

van der Sloot B, ‘A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principles’ (2018) 34 Computer Law & Security Review 539

van der Sloot B, ‘How to assess privacy violations in the age of Big Data? Analysing the three different tests developed by the ECtHR and adding for a fourth one’ (2015) 24 Information and Communications Technology Law 74

Vaz P and Bruno F, ‘Types of Self-surveillance: from abnormality to individuals ‘at risk’’ (2003) 1 Surveillance and Society 272

Viadhynathan S, ‘The rise of the cryptopticon’ (2015) 17 Hedgehog Review

Walker S, ‘Expense, social and moral control. Accounting and the Administration of the Old Poor Law in England and Wales’ (2004) 23 Journal of Accounting and Public Policy 85

Warren S and Brandeis L, ‘The right to privacy’ (1890) 4 Harvard Law Review 193

Whitson J and Haggerty K, ‘Identity theft and care of the virtual self’ (2008) 37 Economy and Society 572

Wright D and Raab C, ‘Privacy principles, risks, and harms’ (2014) 28 International Review of Law, Computers & Technology 277

Yourow H, ‘The margin of appreciation doctrine in the dynamics of European human rights jurisprudence’ (1987) 3 Connecticut Journal of International Law 111

Zimmerman A, ‘Legislating being: The spectacle of words and things in Bentham’s panopticon’ (2008) 3 The European Legacy 72

Zuboff S, ‘Big other: surveillance capitalism and the prospects of an information civilisation’ (2015) 30 Journal of Information Technology 75

Zurawski N, '"I know where you live!" – aspects of watching, surveillance and social control in a conflict zone (Northern Ireland)' (2005) 2 Surveillance & Society 498

Cases

A and others v Secretary of State for the Home Department (2004) UKHL 56

A and others v UK (2009) 49 ECHR 29

A, B, and C v Ireland (2011) 53 ECHR 13

Aksoy v Turkey (1997) 23 ECHR 553

Amann v Switzerland (2000) 30 ECHR 843

Association for European Integration and Human Rights and Ekimdshiev v Bulgaria App no. 62540/00 (ECtHR, 28 June 2007)

Big Brother Watch and Others v UK 58170/13 (ECtHR, 4 November 2017)

Burghartz v Switzerland (1994) 18 ECHR 105

Bykov v Russia App no.4378/02 (ECHR, 10 March 2009)

Chapman v United Kingdom (2001) 33 ECHR 18

de Freitas v Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing [1999] 1 AC 69 the Privy Council

Delcourt v Belgium (1979-80) 1 ECHR 355

Entick v Carrington (1765) 19 St Tr 1029

European Integration and Human Rights and Ekimdzhiev v Bulgaria App no.62540/00 (ECHR, 28 June 2007)

Friedl v Austria (1996) 21 ECHR 83

Gaskin v United Kingdom (1990) 12 ECHR 36

Gillan and Quinton v United Kingdom (2010) 50 ECHR 45

Goodwin v United Kingdom (2002) 35 ECHR 18

Halford v United Kingdom (1997) 14 24 ECHR 523

Halford v United Kingdom (1997) 24 EHRR 523

Handyside v United Kingdom (1979-80) 1 ECHR 737

Herbecq v Belgium 32200/96 and 32201/96 (Commission Decision, 14 January 1998

Huvig v France (1990) 12 ECHR 528

Iordachi v Moldova (2012) 54 ECHR 5

Iordachi v Moldova (2012) 54 ECHR 5

Ireland v UK (1979-80) 2 ECHR 25

Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and others* [2016] EU:C:2016:970

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd and Seitlinger v Minister for communications, marine and natural resources* [2015] EU:C:2015:650

Kennedy v United Kingdom (2011) 52 ECHR 4

Khan v UK (2001) 31 ECHR 45

Klass v Germany (1979-80) 2 ECHR 214

Klass v Germany App no 5029/71 (Commission Decision, 9 March 1977)

Kopp v Switzerland (1999) 27 ECHR 91

Kruslin v France (1990) ECHR 547

Kyrtatos v Greece (2005) 40 ECHR 16

Lane v Facebook 709 F.3d 791 (9th Cir. 2013)

Lawless v Ireland (no 3) (1979-80) 1 ECHR 15

Leander v Sweden (1987) 9 ECHR 433

Liberty and others v GCHQ [2014] UKIPTrib 13_77-H

Liberty v UK (2009) 48 ECHR 1

Liberty v UK (2009) 48 ECHR 1

Lingens v Austria (1986) 8 ECHR 407

Maldovan and others v Romania (no.2) App nos. 41138/98 and 64320/01 (ECtHR, 12 July 2005)

Malone v United Kingdom (1985) 7 ECHR 14

Niemietz v Germany (1996) 16 ECHR 97

Norris v Ireland (1991) 13 ECHR 186

Parliament v Council [2006] 3 CMLR 9

Paul Chambers v Director of Public Prosecutions [2012] EWHC 2157

Peck v United Kingdom (2003) 36 ECHR 41

Petri Sallinen and others v Finland App nos. 50882/99 (ECtHR, 27 September 2009)

PG and JH v United Kingdom (2008) 46 ECHR 51

Pretty v United Kingdom (2002) 35 ECHR 1

Privacy International v Secretary of state for foreign and commonwealth affairs and GCHQ [2016] UKIP Trib 14_85-CH

Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Home Department, GCHQ, SS, SIS [2017] UKIPTRib IPT_15_110_CH

Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, GCHQ, Security Service, and SIS [2016] IPT/15/110 CH

R (on the application of Catt) and R(T) v Association of Chief Police Officers of England, Wales and Northern Ireland [2015] UKSC 9

R (on the application of Daly) v Secretary of State for the Home Department [2001] UKHL 26

R (The National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department & Anor [2018] EWHC 975 (Admin)

R v Preston [1994] 2 AC 130

RE v United Kingdom (2016) 63 ECHR 2

Rotaru v Romania (2000) 8 BHRC 449

S and Marper v United Kingdom (2009) 48 ECHR 50

Secretary of State for the Home Department v Watson MP & Ors [2018] EWCA Civ 70

Silver and others v UK (1983) 5 ECHR 347

Szabó and Vissy v Hungary (2016) 63 ECHR 3

The Sunday Times v United Kingdom (1979) 2 ECHR 245

Uzun v Germany (2011) 53 ECHR 24

Valenzuela-Contreras v Spain (1999) 28 ECHR 483

Weber and Saravia v Germany (2006) ECHR 1173

Zakharov v Russia (2016) 63 ECHR 17

Statutes

Act for the Relief of the Poor 1597

Act of Supremacy 1534

An Act for Taking an Account of the Population of Great Britain, and of the Increase or Diminution thereof 1800

Anti-Terrorism Crime and Security Act 2001

Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37 (ePrivacy Directive)

Council Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54 (Data Retention Directive)

Council Directive 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (Law Enforcement Directive)

Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJL281/31 (Data Protection Directive)

Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (GDPR)

Counter-Terrorism Crime and Security Act 2015

Criminal Justice and Police Act 2001

Criminal Procedure Act of Scotland 1995

Data Retention and Investigatory Powers Act 2014

Draft Communications Data Bill 2012

European Convention on Human Rights 1953

Factory and Workshop Act 1891

Human Rights Act 1998

Intelligence Services Act 1994

Intelligence Services Act 2004

Interception of Communications Act 1985

Investigatory Powers Act 2016

Magistrates Courts Act 1980

Police and Criminal Evidence Act 1984

Police, Public Order and Criminal Justice (Scotland)Act 2006

Poor Law Act 1535

Poor Law Amendment Act 1834

Protection of Freedoms Act 2012

Regulation of Investigatory Powers Act 2000

Security Services Act 1989

Statutes of the Realm 1571

Telecommunications Act 1984

Terrorism Act 2000

Terrorism Act 2000 (Remedial Order) 2011

Terrorism Act 2006

Terrorism Act 2008

The Misuse of Drugs Act 1971

The Police Act 1997

The Wireless Telegraphy Act 2006

Vagabonds Act 1572

Reports

Article 28 Data Protection Working Party, 'Opinion 2/2017 on data processing at work' (8 June 2017) 17/EN WP 249

Birkett Committee, *Report of the Committee of Privy Councillors Appointed to Inquire into the Interception of Communications* (Cmnd 283, 1957)

Council of Europe, *Human Rights Files no.15* (Council of Europe Publishing, 1997)

David Anderson QC Independent Reviewer of Terrorism Legislation, *Report of the bulk powers review* (Cm 9326, 2016)

Delegated Power and Regulatory Reform Committee, *Sixth report of session 2017-19* (2017-19, HL 29)

Departmental Committee on National Registration, *Report of the Sub-Committee Appointed to Consider a System of General Election* (PRO RG 28/4, 1918)

General Register Office, *77th Annual Report of the Register General for 1914* (London: HMSO, 1916)

Home Affairs Committee: Evidence, *Counter-terrorism 17th Report*, (2013-14, HC231)

Home Office, *Draft Investigatory Powers Bill: explanatory notes* (Cm 9152, November 2015)

Home Office, *Equipment interference: draft code of practice* (Crown Publishing, 2016)

Home office, *Secretary of State for the Home Department, Investigatory powers bill: government response to pre-legislative scrutiny* (Cm 9219, 2016)

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

Home Office, *The national security strategy and strategic defence and security review 2015: a secure and prosperous United Kingdom* (Cm 9161, 2015)

Home Secretary, *Interception of communications in the United Kingdom: a consultation paper* (Cm 4368, 1999)

House of Lords Constitution Committee, *Data Protection Bill* (2017-19, HL 31)

Independent Reviewer of Terrorism Legislation, *A question of trust* (Crown, 2015)

Intelligence and Security Council, *Privacy and security: a modern and transparent legal framework* (2014-15, HC 1075)

Joint Committee on Human Rights, *Legislative scrutiny; investigatory powers bill* (2016-17, HL 6, HC 104)

Joint Committee on the Draft Communications Bill, *Draft Communications Data Bill* (2012-13, HL 79, HC 479).

Joint Committee on the Draft Investigatory Powers Bill, *Legislative scrutiny: Draft Investigatory Powers Bill* (2016, HL 93, HC 651)

Ministry of Defence, *Land Operations Volume III – Counter-Revolutionary Operations* A/26/GS Trg Publications/3011 (Ministry of Defence, 1969)

Philip Ward, *Briefing paper: Communications data: the 2012 draft bill and recent developments (No.06373)* (House of Commons Library, 12 June 2015)

Royal Commission, Report from his Majesty's Commissioners for Inquiring into the Administration and Practical Operation of the Poor Laws, (C (1_{st} series) 44, 1834)

Royal United Services Institute for Defence and Security Studies, *A democratic license to operate: report of the independent surveillance review* (RUSI, 2015)

Secretary of State for the Home Department, *Investigatory powers bill: government response to pre-legislative scrutiny* (Cm 9219, 2016)

Select Committee on the Constitution, *Surveillance: citizens and the state* (HL 2008-09, 18-I)

Sir David Omand, Jamie Bartlett, Carl Miller, '#intelligence' (*Demos*, 2012)

The Bichard Inquiry, *The Bichard inquiry report* (2004, HC653)

The RT Hon The Lord Saville of Newdigate, The Hon William Hoyt OC, The Hon John Toohey AC, *Report of the Bloody Sunday Inquiry* (HC 2010-2011, 29-1)

UN Docs

David Kaye, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' A/HRC/29/32 (United Nations, 22 May 2015)

UNCHR, ‘Report of the special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism’ (28 December 2005) E/CN.4/2006/98, 2005

UNGA ‘The Declaration on Measures to Eliminate International Terrorism, in the annex to UN General Assembly Resolution’ (9 December 1994) A/RES/49/60.

UNSC, ‘Res 1368 (2001)’ (12 September 2001) S/Res/1368 (2001)

Newspaper Articles

Atkinson S, ‘How can credit reference agencies catch benefit cheats?’ *BBC News* (London, 10 August 2010)

Ball J, Harding L, Garside J, ‘BT and Vodafone among telecoms companies passing details to GCHQ’ (*Guardian news,* 2 August 2013)

BBC News, ‘Ahmed Saleh kicked off Delta air lines flight’ (*BBC News online,* 23 December 2016)

BBC News, ‘Crowd-sourcing used to trace London riot suspects’ (*BBC News online,* 26 June 2012)

BBC News, ‘Delta hits back against Conservative author Ann Coulter’ (*BBC News online,* 17 July 2017)

Gibbs S, ‘Court sets legal precedent with evidence from Fitbit health tracker,’ (*The Guardian,* 18 November 2014)

Greenwald G and MacAskill E, ‘NSA Prism program taps in to user data of Apple, Google and others’ (*The Guardian,* 7 June 2013)

Guardian News, ‘NSA PRISM program slides’ (*Guardian news,* 1 November 2013)

Hopkins N, Borger J, Harding L, ‘GCHQ: Inside the top secret world of Britain’s biggest spy agency’ (*The Guardian,* 2 August 2013)

Lancaster J, ‘The Snowden files: why the British public should be worried about GCHQ’ (*Guardian news,* 3 October 2013)

MacAskill E, Borger J, Hopkins N, Davies N, Ball J, ‘GCHQ taps fibre-optic cables for secret access to world’s communications’ (*The Guardian,* 21 June 2013)

Sanchez J, ‘Snowden just showed us how big the panopticon really was. Now it’s up to us’ (*Guardian news,* 5 June 2014)

Solon O, ‘Have you given Pokemon Go full access to everything in your Google account?’ (*Guardian News,* 12 July 2016)

Wong J and Lewis P, ‘Facebook gave data about 57bn friendships to academic’ (*The Guardian,* 22 March 2018)

Zezima K, ‘The secret service wants software that detects sarcasm. (Yeah, good luck.)’ (*The Washington Post,* 3 June 2014)

Websites and Other

75 HC Deb 151 (12 March 1985)

Bush G W, ‘Address to the Nation: Address Before a Joint Session of the Congress on the United States Response to the Terrorist Attacks of September 11’ 37 WCPD 1347 (20 September 2001)

Cambridge dictionary online <https://dictionary.cambridge.org/dictionary/english/surveillance>

Clarke R, ‘Introduction to dataveillance and information privacy, and definition in terms’ (*Roger Clarke’s homepage*) <http://www.rogerclarke.com/DV/Intro.html> accessed 14 June 2018

Facebook Statistics (Facebook, 31 March 2018) https://newsroom.fb.com/company-info/

Gallagher R, Greenwald G, ‘How the USA plans to infect “million” of computers with malware’ (The Intercept, 12 March 2014) < https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/> accessed 2 August 2017

Gallagher S, ‘Building a panopticon: the evolution of the NSAs Xkeyscore’ (Arstechnica, 9 August 2013) <https://arstechnica.com/information-technology/2013/08/building-a-panopticon-the-evolution-of-the-nsas-xkeyscore/> accessed 20 June 2018

HC Deb 13 April 2016, vol 68, col 347

HL Deb 25 January 1916, vol 20, col 997

HL Deb 5 July 1915, vol 73, col 135

Lapowsky I, ‘Facebook exposed 87 million users to Cambridge Analytica’ (Wired, 4 April 2018) <https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/> accessed 2 May 2018.

Mann S, ‘The sightfield: visualising computer vision, and seeing its capacity to “See”’ Published as part of 2014 Conference on Computer Vision and Pattern Recognition Workshops<https://pdfs.semanticscholar.org/f4f2/f7a1861d667f068f89eccf99793033851c9c.pdf?_ga=2.3916791.678783471.1525191510-1786373483.1525191510> accessed 1 May 2018.

Manovich L, ‘Software takes command’ (unpublished, 2008) <http://softwarestudies.com/softbook/manovich_softbook_11_20_2008.pdf> accessed 5 July 2017.

OHCHR, The Right to Privacy in a Digital Age (June 30, 2014) <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf>

Richard Watson Lord Bishop of Landaff (SSV representative), A sermon preached before the Society for the Suppression of Vice (‘SSV’) in the Parish Church of St George (3rd May 1804)

Rumsfeld D (Nato Press Conference, Brussels, 6 June 2002) <http://www.nato.int/docu/speech/2002/s020606g.htm> accessed 27 April 2016

Tran M, ‘War on terror – a term that no longer applies’ (The Guardian, 15 January 2009) <https://www.theguardian.com/news/blog/2009/jan/14/war-on-terror-david-miliband-mumbai> accessed 5 April 2018.

Zuckerberg M, 'Thoughts on Beacon' (Facebook, 5 December 2007) <https://www.facebook.com/notes/facebook/thoughts-on-beacon/7584397130/> accessed 7 July 2017.

Zuckerberg M, Facebook founder, speaking at the Crunchie awards in San Francisco (Guardian news, 11 January 2010) <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> accessed 5 September 2016

Chan K, 'Facebook across the Web' (Facebook, 4 December 2008) <https://www.facebook.com/notes/facebook/facebook-across-the-web/41735647130/> accessed 7 July 2017.

Angwin J, Pravis T Jr, 'Facebook lets advertisers exclude users by race' (ProPublica, 28 October 2016) <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race> accessed 16 August 2017.

United States Marine Corps Comments on Joint Open Source Task Force Report and Recommendations'(1992)<http://www.oss.net/dynamaster/file_archive/060324/9906ba66ee5fe750bb8fe5712b1e20e7/92%20Jan%2011%20Steele%20on%20IC%20OSINT.pdf> accessed 11 July 2017.

National Police Chief's Council, 'National Domestic Extremism Unit' (NPCC) <http://www.npcc.police.uk/NationalPolicing/NDEDIU/AboutNDEDIU.aspx> accessed 12 July 2017.

Marquis-Boire M, Greenwald G, Lee M, 'XKeyscore' (The Intercept, 1 July 2015) <https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/> accessed 12 July 2017.

Cagle M, 'Facebook, Instagram, and Twitter provided data access for a surveillance product marketed to target activists of colour' (ACLU, 11 October 2016) <https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target> accessed 13 July 2017.

Oxford English Dictionary (7th edn, Oxford University Press, 2012)

'I like Frank' visit <http://www.blasttheory.co.uk/projects/i-like-frank/> accessed 18 July 2017.

NYU Centre for Data Science, 'How is Pokémon Go collecting data on its users' <http://datascience.nyu.edu/how-is-pokemon-go-collecting-data-on-its-users/> accessed 18 July 2017.

Kamen M, 'Pokémon Go's first sponsored location will be McDonald's – in Japan' (*Wired,* 2016*)* <http://www.wired.co.uk/article/pokemon-gos-first-sponsored-location-will-be-mcdonalds-in-japan> accessed 18 July 2017.

'Notice of objections to February 16, 2016 order compelling Apple Inc. to assist agents in search,' available via <https://www.justsecurity.org/wp-content/uploads/2016/03/FBI-Apple-Apple-Notice-of-Objections.pdf> accessed 17 August 2017.

Quantified Self website, ‘Quantified Self: self knowledge through numbers’ at <http://quantifiedself.com> accessed 21 July 2017.

Wolf G, ‘Know thyself: tracking every facet of life, from sleep to mood to pain 24/7/365’ (*Wired*, 22 June 2007) <https://link.springer.com/content/pdf/10.1007%2Fs13347-016-0215-5.pdf> accessed 20 July 2017

ABI Research, ‘Corporate wellness is a 13 million unit wearable wireless device opportunity’ (ABI Research, 25 September 2013) <https://www.abiresearch.com/press/corporate-wellness-is-a-13-million-unit-wearable-w/> accessed 24 July 2017.

Rosenbach M, Poitras L, Stark H, ‘How the NSA accesses smartphone data’ (*Spiegel online*, 9 September 2013) <http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html> accessed 2 August 2017.

Privacy International, ‘Eyes wide open: special report’ (Version 1.0, Privacy International, 26 November 2013) <https://www.privacyinternational.org/node/301> accessed 27 July 2017

European Commission Fact Sheet, ‘Questions and answers – data protection reform package’ (24 May 2017) <http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm> accessed 31 October 2017

Information Commissioner's Office, 'Key definitions' (*ICO*) <www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/.> accessed 24 June 2018

EMC Infobrief with research and analysis by IDC, 'The digital universe of opportunities: rich data and the increasing value of the internet of things' (*EMC*, April 2014) <https://www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf> accessed 31 July 2017

Big Brother Watch in its written evidence to the Joint Committee on the Draft IP Bill (DIP0007)

Privacy International written evidence to the Joint Committee on the Draft IP Bill (IPB0120)

Home Office written evidence to the Joint Committee on the Draft IP Bill (IPB0146)

LINX written evidence to the Joint Committee on the Draft IP Bill (IPB0097)

Crown Prosecution Service written evidence to the Joint Committee on the Draft IP Bill (IPB0081)

Open Intelligence written evidence to the Joint Committee on the Draft IP Bill (IPB0066)

Liberty written evidence to the Joint Committee on the Draft IP Bill (IPB0143)

John Hopkins foreign affairs symposium presents: the price of privacy: re-evaluating the NSA' (John Hopkins University, 1 April 2014) <https://www.youtube.com/watch?v=kV2HDM86XgI> accessed 30 October 2017

Paul Bernal written evidence to the Joint Committee on the Draft IP Bill (IPB0018)

Graham Smith written evidence to the Joint Committee on the IP Bill (IPB0126)

BT supplementary written evidence to the Joint Committee on the Draft IP Bill (IPB0151)

Matthew Ryder Oral Evidence to the Draft Investigatory Powers Bill (Q186)

Theresa May Oral evidence to the Joint Committee on the Draft IP Bill (Q271)

Eric King oral evidence to the Joint Committee on the Draft Investigatory Powers Bill, Q202

Home Office, Operational case for bulk powers, para 10.7 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf> accessed 24 June 2018.

HC deb 4 November 2015, col 969

William Binney oral evidence to the Joint Committee on the Draft IP Bill (Q239)

Ray Corrigan written evidence to the Joint Committee on the Draft IP Bill (IPB0053)

Paul Bernal supplementary written evidence to the Joint Committee on the Draft IP Bill (IPB0018)

Centre for Technology and Democracy written evidence to the Joint Committee on the Draft IP Bill (IPB0110)

HC Deb 4 November 2015, col 972

Dr Tom Hickman in his written evidence to the Joint Committee on the Draft IP Bill (IPB0039)

Christopher Graham Information Commissioner oral evidence to the Joint Committee on the Draft IP Bill (Q231)

John Perry Barlow, 'Declaration of independence for cyberspace' (*Electronic Frontier Foundation*, February 8 1996) <https://www.eff.org/cyberspace-independence> accessed 16 February 2018

Prime Minister's Office, 'The Queen's Speech 2015' (27 May 2015) <https://www.gov.uk/government/speeches/queens-speech-2015> accessed 5 June 2018

Prime Minister's Office, 'The Queen's Speech 2017' (21 June 2017) <https://www.gov.uk/government/speeches/queens-speech-2017> accessed 14 August 2018

Will Dahlgreen, 'Broad support for increased surveillance powers' (YouGov, 18 January 2015) <https://yougov.co.uk/news/2015/01/18/more-surveillance-please-were-british/> accessed 5 June 2018

Lessig L, 'Laws that choke creativity' (*TED talk*, 15 November 2007) <https://www.youtube.com/watch?v=7Q25-S7jzgs> accessed 18 March 2018