Surveillance Law, Data Retention and Risks to Democracy and Rights

Matthew White

A thesis submitted in partial fulfilment of the requirements of Sheffield Hallam University for the degree of Doctor of Philosophy

October 2018

Abstract

In *Klass and others v Germany*, the first surveillance case before the European Court of Human Rights, it was acknowledged that the threat of secret surveillance posed by highlighting its awareness 'of the danger such a law poses of undermining or even destroying democracy on the ground of defending it.' This thesis considers a form of surveillance, communications data retention as envisioned in Part 4 of the Investigatory Powers Act 2016 and its compatibility with the European Convention on Human Rights. This thesis highlights that communications data is not only just as, if not more intrusive than intercepting content based on what can be retained. It also reveals that communications data is mass surveillance within surveillance. Additionally, this thesis demonstrates that communications data does not just interference Article 8 of the Convention, but a collection of Convention Rights including Articles 9, 10, 11, 14, Article 2 Protocol 4 and potentially Article 6. Each of these rights are important for democracy and Article 8 and privacy underpins them all. Furthermore, this thesis highlights that obligation to retain communications data can be served on anything that can communicate across any network. Taking all factors highlighted into consideration, when assessed for compatibility with the Convention, communications data retention in Part 4 not only fails to be 'in accordance with the law', it fails to establish a legitimate aim, and fails to demonstrate its necessity and proportionality. In establishing that communications data retention as envisaged in Part 4 of the Investigatory Powers Act 2016 is incompatible with the Convention, it demonstrates that it undermines democracy and has sown the seeds for its destruction. Not only would the findings of this thesis create an obstacle to an UK-EU post-Brexit adequacy finding, it would have an impact beyond UK law as many States in Europe and outside seek to cement data retention nationally.

Acknowledgements

I would like to express my very great appreciation to my supervisors, Alan Reid, James Marson and Jamie Grace for their expertise, guidance and support. I would also like to offer my special thanks to my family for their encouragement. Finally, I would also like to thank the late Caspar Bowden who nudged me into writing this thesis in the first place.

Contents

Word Count: 96,716

Chapter 1: Introduction and Methodology

1.1 The Explosion of Data and the Information Overload

In 2014, Susan Gunelius wrote about the data explosion of how much data is created every minute for certain services.[1] This explosion in data lead to Richard Harris predicting that more data will be created in 2017 than the previous 5000 years of humanity.[2] Harris argued that the type of data everyone will create is:

> [E]xpanding rapidly across a wide range of industries: biotech, energy, IoT, healthcare, automotive, space and deep sea explorations, cyber-security, social media, telecom, consumer electronics, manufacturing, gaming, and entertainment.[3]

In 2017, Linnet Taylor, Luciano Floridi, and Bart van der Sloot acknowledged that there were 7.4 billion mobile connections worldwide, 5.5 billion of them in low and middle income countries and 2.1 billion people already online.[4] According to the Office for National Statistics (ONS) Internet Access Quarterly Update, Q1, 89% of adults in the UK had recently used the internet, an increase of 1% from 2016.[5] In 2013, Ofcom acknowledged that:

> The internet is at the heart of how many people communicate, find information and seek entertainment. And more and more devices are becoming internet-enabled. As a result it is becoming increasingly difficult to separate the use of internet services from conventional television, radio and voice communication services – they can all be provided by the same device.[6]

With the Internet of Things (IoT), the digital is spilling over into the analog and merging with it[7] creating an 'onlife' which leads to the 'new experience of a hyperconnected reality within which it is no longer sensible to ask whether one may be online or offline.'[8] This has led to what Mark Andrejevic regards as 'infoglut' or information overload, in which we are in an age

---

[1] Susan Gunelius, 'The Data Explosion in 2014 Minute by Minute – Infographic' (12 July 2014) <https://aci.info/2014/07/12/the-data-explosion-in-2014-minute-by-minute-infographic/> accessed 27 October 2017.

[2] Richard Harris, 'More data will be created in 2017 than the previous 5,000 years of humanity' (23 December 2016) <https://appdevelopermagazine.com/4773/2016/12/23/more-data-will-be-created-in-2017-than-the-previous-5,000-years-of-humanity-/> accessed 27 October 2017.

[3] ibid.

[4] Linnet Taylor, Luciano Floridi, and Bart van der Sloot, 'Introduction: A New Perspective on Privacy' in Linnet Taylor, Luciano Floridi, and Bart van der Sloot (eds) *Group Privacy New Challenges of Data Technologies* (Springer Nature 2017), 3.

[5] Office for National Statistics. 'Internet users in the UK 2017' (19 May 2017) <https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2017> accessed 3 January 2018.

[6] Ofcom, 'Communications Market Report 2013' (1 August 2013) <https://www.ofcom.org.uk/__data/assets/pdf_file/0021/19731/2013_uk_cmr.pdf> accessed 3 January 2018, p259.

[7] Luciano Floridi, 'A Look into the Future Impact of ICT on Our Lives' (2007) The Information Society 23:1 59, 61.

[8] Luciano Floridi, *The Onlife Manifesto Being Human in a Hyperconnected Era* (Springer 2009), 1.

where there is too much information to decipher.[9] From a policing and security perspective, Andrejevic acknowledges that this leads to data collection without limits as it renders all data as potentially relevant, no matter how seemingly trivial, irrelevant, personal or invasive it may seem.[10] This is precisely what this thesis, from the perspective of the legality of communications data retention aims to tackle.

(a) The European Convention on Human Rights, a Bulwark Against Totalitarianism?

> The dossier of private information is the badge of the totalitarian state.[11]

The European Convention on Human Rights (ECHR or Convention Rights) was set up with the primary aim (though not its only one)[12] of creating a type of collective pact against totalitarianism.'[13] From as early as 2004, the Information Commissioner, Richard Thomas warned that the UK was sleep walking into a surveillance society.[14] Jacobs notes that Thomas was referring 'to the increased recording and monitoring of people's behaviour' such as 'data retention for (mobile) phone and email communication.'[15] History appears to have repeated itself with regards to the Investigatory Powers Act 2016 (IPA 2016), the 'most intrusive surveillance law of any democracy in history'[16] as 76% of Britons were completely unaware of the legislation in question.[17] This public and political debate has been overshadowed by the UK's intention to leave the European Union[18] (which will have implications for data protection adequacy, see Chapter 8).

Jacobs preferred the term totalitarian society to surveillance society, and did not confine totalitarianism to brutal physical suppression.[19] For Jacobs, totalitarian societies deliberately 'exert explicit influence and control in private lives.'[20] Jacobs continues that the issue of potential abuse is serious and has to be faced explicitly because preventing totalitarian societies is one of the major challenges of our time.[21] In addition, Jacobs notes that the 'emergence of

---

[9] Mark Andrejevic, *Infoglut: How Too Much Information is Changing the Way We Think and Know* (Routledge 2013), 1-2.
[10] ibid, 36.
[11] *Marcel and Others v Commissioner of Police of the Metropolis and Others* [1991] 2 W.L.R. 1118, [1130].
[12] Maris Burbergs, 'How the right to respect for private and family life, home and correspondence became the nursery in which new rights are born: Article 8 ECHR' in Eva Breams and Janneke Gerards (eds) *Shaping Rights in the ECHR: The Role of the European Court of Human Rights in Determining the Scope of Human Rights* (Cambridge University Press), 318.
[13] Ed Bates, *The Evolution of the European Convention on Human Rights: From Its Inception to the Creation of a Permanent Court of Human Rights* (Oxford University Press, 2010), preface; Luzius Wildhaber, 'Dialogue Between Judges' (2006) <http://www.echr.coe.int/Documents/Dialogue_2006_ENG.pdf> accessed 4 October 2017.
[14] Richard Ford, 'Beware rise of Big Brother state, warns data watchdog' (16 August 2004) <https://www.thetimes.co.uk/article/beware-rise-of-big-brother-state-warns-data-watchdog-hhv3qtwgswk> accessed 3 January 2018.
[15] Bart Jacobs, 'Keeping our Surveillance Society Nontotalitarian' (2009) 1(4) Amsterdam Law Forum <http://amsterdamlawforum.org/article/view/91/165> accessed 3 January 2018.
[16] Liberty, 'State Surveillance' <https://www.liberty-human-rights.org.uk/human-rights/privacy/state-surveillance> accessed 3 January 2018.
[17] Aatif Sulleyman, 'Snooper's Charter: Majority of Public Unaware of Government Online Surveillance' (22 May 2017) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-investigatory-powers-bill-government-online-surveillance-majority-uk-unaware-a7749851.html> accessed 3 January 2018.
[18] Ibid; House of Commons Library, 'Brexit: what happens next?' (30 June 2016) <http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7632> accessed 25 July 2016.
[19] Bart Jacbobs, (n15).
[20] ibid.
[21] ibid.

populist movements in Europe, with their limited care for fundamental civil rights, may be seen as making this matter more urgent.'[22] Dahan concurs[23] and Giddens notes that 'aspects of totalitarian rule are a threat' in advanced societies because surveillance is 'maximized in the modern state.'[24] Zöller notes that liberty dies by inches,[25] the erosion of civil liberties is not an event, but a process (see Chapter 2).

Judge Pettiti in *Malone v UK* noted that:

> The mission of the Council of Europe and of its organs is to prevent the establishment of systems and methods that would allow "Big Brother" to become master of the citizen's private life. For it is just as serious to be made subject to measures of interception against one's will as to be unable to stop such measures when they are illegal or unjustified, as was for example the case with Orwell's character who, within his own home, was continually supervised by a television camera without being able to switch it off.[26]

George Orwell's *1984*[27] has been frequently, and rightly read as a warning against totalitarian systems,[28] the virtual opposite of democracy.[29] This is what the European Court of Human Rights (ECtHR), a judicial organ of the Council of Europe, is tasked with preventing by upholding democratic principles.

(b) Undermining or Destroying Democracy on the Ground of Defending it?

The ECtHR in *Klass v Germany*, the first case on State surveillance before it, acknowledged the threat secret surveillance posed by highlighting its awareness 'of the danger such a law poses of undermining or even destroying democracy on the ground of defending it.'[30] The ECtHR continued that Member States could not adopt whatever measures they deem appropriate.[31] The ECtHR echoed similar sentiments in *Weber and Saravia v* Germany[32] and subsequent rulings.[33] This demonstrates that secret surveillance does not have to reach the threshold of destroying democracy, just undermining it.

This thesis concentrates on only a singular aspect of the many powers found within the IPA 2016, that of communications data retention. This consideration is important because of the

---

[22] ibid.
[23] Michael Dahan, 'The Gaza Strip as Panopticon and Panspectron: The Disciplining and Punishing of a Society' (2013) IJEP 4:3 44.
[24] Anthony Giddens, *The Nation State and Violence: Volume Two of a Contemporary Critique of Historical Materialism* (Cambridge: Polity Press), 310.
[25] Verena Zöller, 'Liberty Dies by Inches: German Counter-Terrorism Measures and Human Rights' (2004) German Law Journal 5:5 469.
[26] *Malone v UK* App no. 8691/79 (ECHR, 2 August 1984), Concurring Opinion of Judge Pettit.
[27] George Orwell, *Nineteen Eighty-Four* (Penguin Classics 2013).
[28] James A. Tyner, 'Self and space, resistance and discipline: a Foucauldian reading of George Orwell's 1984' (2004) Social & Cultural Geography 5:1 129, 130.
[29] Alexandros Mantzaris, ''Totalitarianism', Treason and Containment in Catch-22 (and 1984)' Comparative American Studies An International Journal 9:3 217, 218.
[30] *Klass v Germany* App no. 5029/71 (ECHR, 6 September 1978), [49].
[31] ibid.
[32] *Weber and Saravia v Germany* App no. 54934/00 (ECHR, 29 June 2006), [106].
[33] *Roman Zakharov v Russia* App no. 47143/06 (ECHR, 4 December 2015), [232]; *Dragojević v Croatia* App no. 68955/11 (ECHR, 15 January 2015), [83]; *Szabó and Vissy v Hungary* App no. 37138/14 (ECHR, 12 January 2016), [57].

UK's international influence on other countries surveillance laws.[34] Roger Clarke has argued that data retention arguably 'represents a greater threat to democracy than it does to criminals.'[35] He continued that data retention, a form of mass surveillance applies the 'you're all guilty—we're just not sure what of yet' tenet and up until 2001 'democratic countries decried such attitudes as being a defining characteristic of un-free nations such as East Germany under the Stasi.'[36] The Stasi archive includes '69 miles of shelved documents, 1.8 million images, and 30,300 video and audio recordings.'[37] Bernal also regards data gathering such as retention fitting more closely with the Stasi and Romania's Securitate,[38] and fits the definition of a police state.[39]

The term 'police state' was used as a means of conceptualising emerging totalitarian regimes.[40] The ECtHR in *Klass* noted that '*powers of secret surveillance of citizens*, characterizing as they do *the police state*, are *tolerable under the Convention only in so far as strictly necessary* for safeguarding the democratic institutions (author's emphasis).'[41] The case of *Klass* concerned the interception of telecommunications, which demonstrates that the ECtHR does not confine police states to Nazi Germany or Stalin's United States of Soviet Russia (USSR) i.e. secret police dragging people from their homes at night,[42] and the 'repression of public liberties, the elimination of political exchange, limiting freedom of speech, abolishing the right to strike, freezing wages etc.'[43] The ECtHR's understanding is more akin to including the electronic police state, coined by Jim Davis, which aims to control technology, information and the people who use it.[44] For Logan, the electronic police state is the quiet, unseen use of 'electronic technologies to record, organize, search and distribute forensic evidence against its citizens.'[45] Logan continues that 'every surveillance camera recording, every email you send, every Internet site you surf, every post you make, every check you write, every credit card swipe, every cell phone ping…are held in searchable databases, for a long, long time.'[46] In 2008, Logan conducted a study of police states, (including a State's ability to retain communications

[34] -- 'New law would force Facebook and Google to give police access to encrypted messages' *The Guardian* (London, 14 July 2017) <https://www.theguardian.com/technology/2017/jul/14/new-law-would-force-facebook-and-google-to-give-police-access-to-encrypted-messages?CMP=share_btn_tw> accessed 3 January 2018; James Vincent, 'The UK Now Wields Unprecedented Surveillance Powers – Here's what it means' *The Verge* (Manhattan, New York City, 29 November 2016) <https://www.theverge.com/2016/11/23/13718768/uk-surveillance-laws-explained-investigatory-powers-bill> accessed 8 January 2018.
[35] Roger Clarke, 'Data retention as mass surveillance: the need for an evaluative framework' (2015) International Data Privacy Law 5:2 121.
[36] ibid, 127.
[37] Charley Locke, 'A Rare Look at the Archives of the German Secret Police' *Wired* (San Francisco, California, 11 June 2017) <https://www.wired.com/2017/05/adrian-fish-the-stasi-archives/> accessed 4 January 2018.
[38] Paul Bernal, 'Data gathering, surveillance and human rights: recasting the debate,' (2016) Journal of Cyber Policy 1:2 243, 259-260.
[39] HL Deb 27 November 2001 vol 629, col 253.
[40] Markus Dirk Dubber and Mariana Valverde, *The New Police Science: The Police Power in Domestic and International Governance* (Stanford University Press 2006), 36.
[41] *Klass*, (n30), [42].
[42] Jonathan Logan, 'The Electronic Police State: 2008 National Rankings' (2008) <https://secure.cryptohippie.com/pubs/EPS-2008.pdf> accessed 4 January 2018.
[43] Pablo González Casanova, *Latin America Today* (United Nations University Press 1993), 233.
[44] Jim Davis, '"Police Checkpoints on the Information Highway' (1994) Computer underground Digest 6:72.
[45] Jonathan Logan, (n42).
[46] ibid.

data) and out of 52, England and Wales was ranked 5th[47] the highest amongst Western democracies. In 2010, the UK as a whole was overtaken by the USA and was ranked 6th.[48]

Logan's assessment, of course, occurred before National Security Agency (NSA) contractor, Edward Snowden revealed for example, that the UK's spy agency, GCHQ, gained access to the 'network of cables which carry the world's phone calls and internet traffic' and 'has started to process vast streams of sensitive personal information'[49] under their TEMPORA programme.[50] Snowden's revelations[51] have put surveillance powers and privacy into the spotlight, resulting in a series of cases, both domestically[52] and internationally.[53] Nor could the assessment consider the Intelligence and Security Committee's (ISC) (which examines the policy, administration and expenditure of the UK's intelligence agencies)[54] avowal of intrusive powers such as bulk personal data sets (BPD)[55] (sets of personal information about a large number of individuals, the majority of whom will not be of any interest to MI5)[56] or the Home Office's avowal of s.94 of the Telecommunications Act 1984 used to collect communications data in bulk.[57] The Snowden revelation did not prevent 'the continuation and expansion of surveillance powers'[58] by the UK. This highlights why the UK's surveillance regime was closely behind less democratic[59] States such as North Korea and China. This was even before the above-mentioned revelations, which only serves to highlight the necessity of a rigorous assessment of data retention's legality under the ECHR, which had already been invalidated at an EU level in *Digital Rights Ireland*.[60]

Just as totalitarianism is the opposite of democracy, surveillance itself is its opposite,[61] a menace,[62] a sinister force that threatens personal freedoms.[63] Kevin D. Haggerty and Mina

---

[47] ibid.
[48] Jonathan Logan, 'The Electronic Police State: 2010 National Rankings' (2010) <https://secure.cryptohippie.com/pubs/EPS-2008.pdf> accessed 4 January 2018.
[49] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, 'GCHQ taps fibre-optic cables for secret access to world's communications' *The Guardian* (London, 21 June 2013) <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> accessed 5 January 2018.
[50] -- *Der Spiegel* (Hamburg) <http://www.spiegel.de/media/media-34103.pdf> accessed 5 January 2018.
[51] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, (n49).
[52] Franziska Boehm and Mark D. Cole, 'Data Retention after the Judgement of the Court of Justice of the European Union' (30 June 2014) <http://www.zar.kit.edu/DATA/veroeffentlichungen/237_237_Boehm_Cole-Data_Retention_Study-June_2014_1a1c2f6_9906a8c.pdf> accessed 31 May 2018, p14-18.
[53] Carly Nyst, 'At last, the data giants have been humbled' *The Guardian* (London, 7 October 2015) <http://www.theguardian.com/commentisfree/2015/oct/07/data-giants-internet-legal-facebook-google> accessed 31 May 2018.
[54] Intelligence and Security Committee, 'About the Committee' <http://isc.independent.gov.uk/> accessed 31 May 2018.
[55] Intelligence and Security Committee, *Privacy and Security: A modern and transparent legal framework* (2014, HC 1075), 151-163.
[56] MI5, 'Bulk Personal Datasets' <https://www.mi5.gov.uk/bulk-data> accessed 31 May 2018.
[57] Home Office, *Draft Investigatory Powers Bill* (Cm 9152 2015), 36(b).
[58] Arne Hintz and Lina Dencik, 'The politics of surveillance policy: UK regulatory dynamics after Snowden' (2016) Internet Policy Review 5:3 1, 5.
[59] Juliet Lapidos, 'The Undemocratic People's Republic of Korea' *Slate* (New York City, 1 April 2009) <http://www.slate.com/articles/news_and_politics/explainer/2009/04/the_undemocratic_peoples_republic_of_korea.html> accessed 4 January 2018.
[60] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECR I-238.
[61] Kevin D. Haggerty and Mina Samatas, 'Surveillance and democracy: an unsettled relationship' in Kevin D. Haggerty and Mina Samatas (eds), *Surveillance and Democracy* (Routledge-Cavendish (2010), 1.
[62] *Roman Zakharov*, (n33), [171].
[63] Kevin D. Haggerty and Mina Samatas, (n61).

Samatas ask what could be more 'self-evident that the fact that *surveillance curtails personal freedoms*, *inhibits democracy*, and *ultimately leads to totalitarianism* (author's emphasis)?'[64] Schwartz argued that the widespread, silent collection of personal information in cyberspace 'is bad for the health of a deliberative democracy' because it 'cloaks in dark uncertainty the transmutation of Internet activity into personal data that will follow one into other areas and discourage civic participation.'[65] Schwartz continued that it also has a negative impact on individual self-determination, making it difficult to engage in the necessary thinking out loud and deliberation with others upon which choice-making depends.[66] Caspar Bowden argued that it was 'incompatible with human rights in a democracy to collect all communications or metadata all the time indiscriminately.'[67] This is important as the ECtHR has a role in enhancing democracy[68] and maintaining and promoting the ideals and values of a democratic society.[69] Consideration of data retention under the ECHR becomes all the more pertinent as the UK has voted to leave the European Union (EU) and in the House of Commons have voted against (the House of Lords disagreeing)[70] retaining the Charter of Fundamental Rights (CFR) in UK law after exit day.[71] This thesis will highlight the various ways in which communications data retention is incompatible with it. In doing so, this thesis will demonstrate that not only does data retention severely undermine democracy, it paves the way for its total destruction.

1.2 Research Aims

The principal aim of this thesis is to examine the compatibility of data retention found within Part 4 of the IPA 2016 with various rights set out in the ECHR.

1.3 Research Questions

In order to fulfil the research aims, a series of questions are asked in build up, such as whether communications data retention poses an equally, if not more serious interference with Convention Rights based on the type of data retained. Furthermore, it will be sought out, which Convention Rights are engaged by communications data retention. Moreover, the question will be asked as to whether communications data retention should be regarded as surveillance.

---

[64] ibid.
[65] Paul M. Schwartz, 'Privacy and Democracy in Cyberspace' (1999) Vand. L. Rev. 52 1607, 1701.
[66] ibid.
[67] Caspar Bowden, 'Privacy and Security Inquiry: Submission to the Intelligence And Security Committee of Parliament' (7 February 2014) <https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/public-evidence/12march2015/20150312-P%2BS-043-Bowden.pdf?attachauth=ANoY7cqU8inv9fTxZ5MVi5GPhH0Z2u9gkKE7yMB3iOOO89VdSiEN3jI_Ak_xqpbYL1eQHrmbf5djj_q8ZnEpOgM8X-oweDJFf2RmI0I-O9mSIsTDPblG9aNZbdSghnH3hjSFNeyj0idMFJxlPGsqFwiOJiQfItgKrRlkNim0nEl2X5UoLhXHm-05_0t75ZdO06d_S6o1OB_dfabXLGl1xCuUmgiwRsOKcn81egRMDl8CfDIO0EedX3OjJPuD7X2uVYQqYeC8u_ddz3neWhhIzB-70lTFQLBlcw%3D%3D&attredirects=0> accessed 4 January 2018, para 7.
[68] Alastair Mowbray, 'Contemporary aspects of the promotion of democracy by the European Court of Human Rights' (2014) European Public Law 20:3 469.
[69] *Soering v UK* App no. 14038/88 (ECHR, 7 July 1989), [87].
[70] Ben Kentish, 'House of Lords defeats government plans to scrap EU rights charter after Brexit' *The Independent* (London, 23 April 2018) <https://www.independent.co.uk/news/uk/politics/brexit-latest-eu-rights-charter-uk-government-house-of-lords-withdrawal-bill-a8318731.html> accessed 31 May 2018.
[71] Ben Kentish, 'Brexit: MPs vote against including European fundamental rights charter in UK law' *The Independent* (London, 16 January 2018) <https://www.independent.co.uk/news/uk/politics/brexit-mps-vote-against-including-european-fundamental-rights-charter-in-uk-law-a8162981.html> accessed 16 January 2018; s.5(4) of the EU (Withdrawal) Act 2018.

Additionally, it will be necessary to ascertain what services can communications data retention obligations can be imposed upon. Finally, all such answers to these questions aids in the determination as to whether Part 4 of the IPA 2016 is compatible with identified Convention Rights.

1.4 Methodology

The methodology for this thesis is one of a doctrinal analysis which:

> [P]rovides a systematic exposition of the rules governing a particular legal category, analyses the relationship between rules, explains areas of difficulty and, perhaps, predicts future developments.[72]

This analysis will be informed by other factors,[73] making it interdisciplinary, which is a convergence of different areas of academic study.[74] Chapter 3 considers the intrusiveness of communications data, and Chapter 5 which considers data retention as secret surveillance within surveillance. The ECtHR's doctrine of a 'living instrument' in which the ECHR must be interpreted in the light of present-day conditions[75] becomes crucial in this regard as a guide for interpretation. This is aided by using a fairly creative interpretation[76] of the ECHR to argue that communications data retention is just as serious (if not more) of an interference as interception or how data retention interferes with Convention Rights other than the obvious Article 8. This creative interpretation is now supported by the ECtHR's interpretation of the ECHR with regards to communications data being regarded as equally intrusive as content. This creative approach and the use of the living instrument will also be used to make future predictions, such as data retention obligations encompassing much more than just Internet Service Providers (ISPs), phone networks, web-based services and apps, but everyday interconnected devices. This approach is consistent with the ECHR in that the ECtHR takes 'a pragmatic, common-sense approach rather than a formalistic or purely legal one.'[77] Thus, this thesis will not be overly rigid, but not too flexible to extend beyond acceptable parameters.

1.5 Original Contribution to Knowledge

This thesis will make an original contribution to knowledge in a variety of ways. Firstly, it will highlight that communications data retention is at least, as equally as serious in terms of interference, as interception. This will also highlight the social value of privacy which is then utilised to inform the interpretation of the ECHR.

Secondly, the importance of Article 8 ECHR for democracy in that it underpins many Convention Rights (Articles 9-11), which are, in and of themselves, crucial for democracy. It will also contribute to knowledge by highlighting the implications of data retention for Article 6 ECHR. Additionally, it will demonstrate that the nature of communications data retention in

---

[72] Dennis Pearce, Enid Campbell and Don Harding, *Australian Law Schools: A Discipline Assessment for the Commonwealth Tertiary Education Commission 1987*.
[73] Oliver Wendell Holmes Jr, 'The Path of the Law' (1897) Harv L Rev 10:8 457, 465–6.
[74] Douglas Vick, 'Interdisciplinarity and the Discipline of Law' (2004) 31 JL & Soc 163, 164.
[75] *Tryer v United Kingdom* App no. 5856/72 (ECHR, 25 April 1978), [31].
[76] Alastair Mowbray, 'Creativity of the European Court of Human Rights' (2005) Human Rights Law Review 5:1 57, 79.
[77] *Botta v Italy* App no. 21439/93 (ECHR, 24 February 1998), [27].

relation to Article 14, fails to discriminate between those who are in a substantially different position and also the possibility biased data to be generated and retained. Moreover, it will for the first time, consider how communications data retention affects freedom of movement found within Article 2 Protocol 4.

Thirdly, linking to the first contribution, this thesis will highlight the far-reaching implications of the IPA 2016 in terms of *who* can be obligated to retain, and *what* can be retained. It will be demonstrated that data retention obligations have moved on from traditional telephone providers and ISPs to websites, any type of network, any device and many more, including Internet of Things (IoT) objects. This is due to the redefinition of telecommunications operators and demonstrates that data retention has to now be considered in terms of any device that can connect to a network or can communicate. It is only then, the far-reaching implications of the IPA 2016 can begin to be realised as browsing habits, thoughts, feelings, movements and other activities will be subject to a continuous 12-month retention period. This will eventually turn one's city, home and oneself into a Panopticon. Additionally, when one considers who can be obligated to retain what, it becomes clear that communications data retention poses at least an equally serious interference with Convention Rights as other surveillance methods such as interception, when sensitive data such as passwords, sexual preferences, religion and political persuasions would be retainable. Further insight is given to the unlimited types of communications data that can be retained either through its generation or vague terminology by using the examples of Big Data and neurotechnologies which produce mind data. The ability to penetrate thoughts would literally create CCTV for inside one's head. This thesis highlights that the who can be served with a retention notice, and what data can be retained has not yet been fully appreciated.

Fourthly, this thesis will contribute to the debate on surveillance by arguing that communications data retention is mass secret surveillance within surveillance by changing the way surveillance is currently understood.

Fifthly, this thesis will be the first in depth analysis of communications data retention that takes consideration beyond Articles 8 and 10, and questions the very existence of data retention. Not only will the legality of Part 4 of the IPA 2016 be scrutinised, but also whether it serves a legitimate aim, and whether it is necessary and proportionate. This thesis will highlight, none of these requirements are satisfied. This thesis contributes further by asking deeper questions than general proportionality in querying the necessity of whom can be obligated to retain, and what can be retained, whether such measures are relevant and sufficient, whether this is the least restrictive measure used. This line of enquiry demonstrates that consideration under the ECHR goes beyond that under the CFR and highlights ways in which the CFR could be enriched by the ECHR.

Sixthly, not only will this thesis highlight the many ways in which communications data retention is incompatible with various Convention Rights, but how it also potentially threatens the presumption of innocence, fairness, increases the possibility of self-incrimination and threatens legal professional privilege, guaranteed by Article 6.

Seventhly, this thesis will highlight that data retention is discriminatory, contrary to Article 14, and even the Court of Justice of the European Union's (CJEU) approach would still be discriminatory and contrary to Article 14.

1.6 Chapter Structure

This thesis is broken down into 8 Chapters, the introduction and methodology being Chapter 1. Chapter 2 briefly considers the legal and political origins of data retention from the 1993 ILETs report, to the IPA 2016 and the milestone judgment of *Digital Rights Ireland* which invalidated the DRD for its incompatibility with the CFR.

Chapter 3 demonstrates that communications data retention is just as, if not more serious of an interference with private life as the interception of content, thus arguing for equivalent safeguards. This position has now been supported by the ECtHR in the recent *Big Brother Watch* case. This is done so by first discussing what communications data is, and where it comes from. This leads to the consideration of the main types of communications data found within the IPA 2016 i.e. Internet Connection Records, Entity and Events Data and the requirement to retain all or any description of data (with examples). It also highlights that the types of data to be retained extends beyond what was required by EU law. This Chapter also highlights the implications of Big Data retention and the social value of privacy.

Chapter 4 demonstrates that data retention is not just a privacy or even an Article 8 issue, but involves numerous fundamental rights and democracy itself. This is explored through not only explaining why data retention interferes with Article 8, but Articles 9-11, Article 14, 6 and Article 2 Protocol 4 and the corresponding rights contained in the CFR (which are meant to be equal to or greater than the ECHR protection). All such rights are in their own right, important for democracy, and Article 8 underpins them. It also importantly highlights a running theme throughout this thesis, data retention, creates a chilling effect on the exercise of fundamental rights. Chapter 5 argues that data retention is a form of mass secret surveillance within surveillance (which also creates a chilling effect) by demonstrating that not only is it Panoptic (knowing of the possibility of being watched), but also Panspectric (being watched unawares). It argues that data retention would fall short of David Lyon's definition of surveillance hence why a new understanding is important. The idea that data retention is surveillance is supported by not only by literature, but by UK, ECHR and EU law. This Chapter also highlights that government and corporations are working in synergy to collectively spy on the populous for their own purposes (surveillance within surveillance). This further strengthens the argument that data retention should receive the same safeguards interception.

Chapter 6 discusses the services obligated to retain communications data. This Chapter details how the obligation has extended from ISPs to now cover any device that transmits a signal (such as apps, websites, Internet of Things devices etc), highlighting that erosion of liberties is done so by inches. Data from your streets, your home and even your body is subject to retention notices. Once again this demonstrates that UK law has taken a step further than EU law in this regard. Building on the previous Chapters, Chapter 7 asks the important question whether data retention in the IPA 2016 is compatible with the rights set forth in the ECHR mentioned in Chapter 4. Since *Digital Rights Ireland* the UK was of the positon that data retention on the grounds of national security are outside the scope of EU law. Whether or not this proves to be the case, this is within the scope of the ECHR, and its consideration becomes crucial. Given the scale of who can be obligated to retain, the types of data to retain, the rights they affect, a full assessment under the ECHR is required. Article 8 is used as a template for the qualified rights because a violation of 8 *ipso facto* violates the others, even when separate considerations/justifications are considered with each. Data retention is tested on its legality, necessity and proportionality. Data retention is also tested on its compliance with Article 6 and

14. This Chapter also highlights deficiencies in the CJEU's ruling in *Tele2 and Watson*[78] and how an interpretation of the ECHR can remedy this (also in terms of data protection).

Chapter 8 concludes that data retention in the IPA 2016 is not only incompatible with various rights set out in the ECHR, it is also incompatible with democracy for reasons that it goes much further than the DRD and that it certainly undermines it and paves the way for its destruction. Another important point to consider is that if the UK leaves the EU, it becomes a third-country, and the issue of transferring personal data outside of the EU to the UK can only occur if the UK satisfies a finding of adequate data protection laws. Given that Chapter 7 demonstrates that just one provision of the IPA 2016 is incompatible various rights in the ECHR, it would be unlikely that the European Commission would regard UK laws as adequate (if the CFR is to be regarded as equal to or greater than), and just like the case of *Schrems*,[79] this would put a halt to data transfer from the EU to the UK.

[78] Joined Cases C‑203/15 and C‑698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-970.
[79] Case C‑362/14 *Schrems* [2015] ECR-I 650.

Chapter 2: An Introduction to Communications Data Retention and its illegality

2. Introduction

This Chapter is an informative overview which seeks to introduce the notion of communications data retention within the European Union (EU) and UK context. The first task is one of defining communications data retention. It is then important to consider the history of data retention proposals, and to highlight that it was the UK that was the main driving force behind data retention laws at national and EU level. Further to this, it will also be highlighted that acts of terrorism have served as a pretext (even if a genuine reason) for data retention when prior attempts had failed. This demonstrates the post 9/11 effect where politicians ultimately overlook the important human rights aspects in the pursuit of perceived security. The reactions from the political dimension is met with judicial restraint as seen by courts of EU Member States and the Court of Justice of the European Union (CJEU) itself in ruling that the Directive 2006/24/EC (the Data Retention Directive, DRD) was invalid for its incompatibility with the Charter of Fundamental Rights (CFR) and subsequent ruling banning general and indiscriminate data retention across the EU. This Chapter analyses the UK's response in depth to data retention through the Investigatory Powers Act 2016 (IPA 2016).

2.1 What is Communications Data Retention?

Communications data retention is as 'a method of data preservation over a certain period of time which is thus available for retroactive investigations into electronic communications by competent authorities.'[1] The types of data that can be retained will be discussed fully in Chapter 3, but it is generally described as the 'who (e.g. David Smith), where (e.g. outside Parliament Square), when (e.g. 21:00 BST) and how (e.g. via hotmail.com through a browser or app) of a communication (e.g. e-mail message).'[2]

2.2 Retention in its infancy

Demands for communications data retention can be traced back to the 'International Law Enforcement and Telecommunications Seminars' (ILETS).[3] ILETS was founded by the Federal Bureau of Investigations (FBI) and has police and security agents from up to 20 countries.[4] Following this, the EU Council of Justice and Home Affairs (JHA) Ministers adopted a Resolution in November 1993, (which was not published) which called upon experts to compare the needs of the EU with regards to the interception of telecommunications 'with those of the FBI.'[5] More requirements were formulated by the FBI and adopted by ILETS in 1994 which formed the basis of a second EU Resolution on the interception of

[1] Kristina Irion, 'Accountability unchained: Bulk Data Retention, Preemptive Surveillance, and Transatlantic Data Protection' in Marc Rotenberg, Julia Horwitz and Jeramie Scott (eds), *Privacy in the Modern Age The Search for Solutions* (New Press 2015), 80, n6.
[2] Matthew White, 'Protection by Judicial Oversight, or an Oversight in Protection?' (2017) Journal of Information Rights, Policy and Practice 2:1 1.
[3] Chris Jones and Ben Hayes, 'The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy' (2013), <http://www.statewatch.org/news/2013/dec/secile-data-retention-directive-in-europe-a-case-study.pdf> accessed 23 May 2017, p6, n7.
[4] Duncan Campbell, 'Intercepting the Internet' *The Guardian* (London, 29 April 1999) <https://www.theguardian.com/technology/1999/apr/29/onlinesupplement3> accessed 31 May 2018.
[5] --Draft Council Resolution on the Interception of Telecommunications, 10090/93 (16 November 1993) <http://database.statewatch.org/e-library/1994-jha-k4-03-06.pdf> accessed 23 May 2017.

telecommunications adopted in January 1995,[6] which had 30 requirements.[7] These 30 requirements set out cooperative obligations of telecommunications companies with law enforcement agencies. In the 1999 ILETS report,[8] a new issue was discovered, notably with the Directive 97/66/EC which made retention of communications data possible only for billing purposes. The action required was 'to consider options for improving the retention of data by Communication Service Providers.'[9] This would eventually lead to Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector, the e-Privacy Directive (e-PD).

2.3 Passage of the e-Privacy Directive

In the initial proposal stages, Article 15(1) of the e-PD, the European Commission (Commission) made no mention of data retention.[10] This was due to it merely being an update of the pre-e-PD.[11] In light of the 9/11 attacks, Article 15(1) was extended to include the retention of data for a *limited period* for *certain major public security interests* (author's emphasis).[12] Statewatch believed this was demanded by former USA President, George W. Bush.[13] The *suggestion* from the White House was to '[r]evise draft privacy directives that call for mandatory destruction to permit the retention of critical data for a reasonable period (author's emphasis).[14] This was in actual fact a *proposal* in *response* to the Belgian Prime Minister (author's emphasis). Moreover, the European Parliament (EP), in the strongest terms opposed this form of retention, in that they urged its use *must* be entirely exceptional, based on specific comprehensible law, authorised by judicial or other competent authorities for *individual* cases and be consistent with the European Convention on Human Rights (ECHR) (author's emphasis).[15] Furthermore, the EP noted that that 'a general data retention principle

[6] Chris Jones and Ben Hayes, (n3), p6.
[7] Council Resolution of 17th January 1995 on the lawful interception of telecommunications, OJ 1996 C 329/01 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:1996:329:FULL:EN:PDF> accessed 23 May 2017.
[8] ILETS Report (1999) <http://www.statewatch.org/news/2001/may/ILETS99-report.doc> accessed 23 May 2017.
[9] ibid.
[10] Commission, Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector' COM(2000) 385 final.
[11] Statewatch, 'Data or data protection in the EU?' <http://www.statewatch.org/news/2001/sep/dataprot.pdf> accessed 23 May 2017.
[12] Council of the European Union, Common Position adopted by the Council on 28 January 2002 with a view to the adoption of the Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, Statement of Reasons, (29 January 2002), <http://data.consilium.europa.eu/doc/document/ST-15396-2001-REV-2-ADD-1/en/pdf> accessed 23 May 2017; Council of the European Union, Working Party on Telecommunications, Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, (16 November 2001) <http://www.statewatch.org/news/2001/nov/13883.pdf> accessed 23 May 2017, 21.
[13] Statewatch, 'European Parliament and EU governments on a collision course over the retention of data (telecommunications surveillance)' <http://www.statewatch.org/news/2001/nov/15eudata.htm> accessed 23 May 2017.
[14] James J. Foster, 'United States Mission to the European Union, Proposals For US-EU Counter-Terrorism Cooperation' (16 October 2001) <http://www.statewatch.org/news/2001/nov/06Ausalet.htm> accessed 23 May 2017.
[15] Marco Cappato,'European Parliament, 2nd Report on the proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector' (24 October 2001) <http://www.statewatch.org/news/2001/nov/cappato.pdf> accessed 23 May 2017, p29.

must be forbidden' and that 'any general obligation concerning data retention' is contrary to the proportionality principle.[16]

However, as noted above, the 9/11 attacks on the World Trade Centre had occurred,[17] which led to the Commission accepting the additional sentence of Article 15(1)[18] the EP had an opportunity to halt this addition, which initially was the case on November 2001, but eventually reversed its position on May 2002.[19] Data retention was opposed by 40 civil liberties organisations to vote against the retention of communications data,[20] the Article 29 Data Protection Working Party (WP29),[21] the European Data Protection Commissioners, [22] the International Chamber of Commerce (ICC), European Internet Services Providers Association (EuroISPA), the US Internet Service Provider Association (USISPA), the All Party Internet Group (APIG)[23] and at the G8 Tokyo Conference.[24] With the EU accepting UK's data retention proposal, it highlights something that members of the UK government denied any plans of, and as Judith Rauhofer notes 'the UK had managed to obtain an enabling provision which would allow member states' to obligate data retention'[25] demonstrating it was the UK that was more influential than the US in this regard.

2.4 Data Retention within the UK and other EU Member States

Prior to the adoption of the e-PD, in the UK, the National Crime and Intelligence Service (NCIS) made a submission (on behalf of the Mi5/6, GCHQ etc) to the Home Office on data retention laws.[26] Blanket data retention was preferred and was ironically noted that a targeted approach would be a 'greater infringement on personal privacy.'[27] Lord Cope noted that 'vast banks of information on every member of the public can quickly slip into the world of Big

---

[16] Abu Bakar Munir and Siti Hajar Mohd Yasin, 'Retention of communications data: A bumpy road ahead' (2004) The John Marshall Journal of Computer & Information Law 22:4 731, 734; Clive Walker and Yaman Akdeniz, 'Anti-Terrorism Laws and Data Retention: War is over?' (2003) Northern Ireland Legal Quarterly 54:2 159, 167.

[17] Judith Rauhofer, 'Just Because You're Paranoid, Doesn't Mean They're Not After You: Legislative Developments in Relation to the Retention of Communications Data' (2006) SCRIPTed 3 322, 331.

[18] Statewatch, 'EU: Final decision on surveillance of communications European Commission sells-out, European Parliament vote due in May, January-February 2002, vol 12 no 1' <http://www.statewatch.org/news/2002/may/05Asurv.htm> accessed 23 May 2017.

[19] Statewatch, 'European Parliament caves in on data retention' (30 May 2002) <http://www.statewatch.org/news/2002/may/10epcavein.htm> accessed 23 May 2017; A breakdown of the voting can be seen here - Statewatch, 'The vote in the European Parliament to accept data retention and surveillance by the law enforcement agencies: an analysis' <http://www.statewatch.org/news/2002/may/15epvote.htm> accessed 23 May 2017.

[20] Statewatch, 'Coalition asks European Parliament to vote against data retention' '(23 May 2002) <http://www.statewatch.org/news/2002/may/09coalition.htm> accessed 23 May 2017; The letter can be viewed here: 22 May 2002<http://gilc.org/cox_en.html> accessed 23 May 2017.

[21] Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime' (22 March 2001) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp41_en.pdf> accessed 23 May 2017, page 7.

[22] Statement of the European Data Protection Commissioners, (11 September 2002) <http://www.fipr.org/press/020911DataCommissioners.html> accessed 23 May 2017.

[23] Abu Bakar Munir and Siti Hajar Mohd Yasin, (n15), p746-749.

[24] G8 Government Industry Workshop on Safety and Security in Cyberspace, (May 2001) <http://cryptome.org/g8-isp-e-spy.htm> accessed 23 May 2017.

[25] Judith Rauhofer, (n17), 331.

[26] Roger Gasper, NCIS submission on data retention law: Looking to the future – clarity on communications data retention law' (21 Aug 2000) <https://cryptome.org/ncis-carnivore.htm> accessed 26 May 2017.

[27] ibid, para 3.1.5.

Brother.'[28] However, Charles Clarke, the then junior Home Office Minister, and Patricia Hewitt, an 'E-Minister' both made the claim such plans would not come into fruition.[29] When questioned about the NCIS's proposals, Hewitt maintained that Charles Clarke and herself disagreed with said proposals and said that it should not be implemented.[30]

But as the previous section noted, the UK did intend to allow itself the power to obligate data retention, and did by using the EU as a proxy. The first law to formalise data retention was under the controversial[31] Part 11 of the Anti-terrorism, Crime and Security Act 2001 (ATCSA 2001) (now omitted by Schedule 10(62) of the IPA 2016). This came into force three months after the 9/11 attacks.[32] This allowed for the voluntary (and if need be mandatory) retention of communications data by communication service providers (CSPs). During the House of Lords debates on ATCSA 2001, Lord Rooker ironically noted that Part 11 was not to be used as generalised [fishing] expeditions[33] when this is exactly how data retention is described.[34] Lord Phillips correctly stated that 'we cannot defend our values by suspending them.'[35] The then Assistant Commissioner to the Information Commissioner Jonathan Bamford observed that 'Part 11 isn't necessary, and if it is necessary it should be made clear why.'[36] The Earl of Northesk was more vocal in criticism, not only highlighting the reversal in the UK's position on retention, but noting that 'there is no evidence whatever that a lack of data retained has proved an impediment to the investigation of the atrocities' on 9/11.[37]

It has been suggested that data retention was possible from as early as 1984 via s.94 of the Telecommunications Act 1984,[38] which may explain how it was possible to retain data in the aftermath of 9/11.[39] Member States such as France and Belgium had, like the UK adopted data retention provisions prior to the e-PD[40] with Belgium adopting prior to 9/11.[41] This demonstrates data retention was not something that was brought about by the e-PD, but could be used as justification for such measures.

---

[28] Kamal Ahmed, 'Secret plan to spy on all British phone calls' *The Guardian* (London, 3 December 2003) <https://www.theguardian.com/uk/2000/dec/03/kamalahmed.theobserver> accessed 26 May 2017.
[29] Caspar Bowden, 'CCTV for inside your head Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation' (2001) <http://europe.rights.apc.org/eu/cctv_for_the_head.html> accessed 23 May 2017; Judith Rauhofer, (n17), 228; Patricia Hewitt and Charles Clarke, Joint letter to Independent on Sunday, 28 Jan 2000.
[30] Trade and Industry Committee, *UK Online Reviewed: the First Annual Report of the E-Minister and E-Envoy Report* (HC 66 1999-2000), Q93.
[31] Caspar Bowden, (n29).
[32] Judith Rauhofer, (n17), 331.
[33] HL Deb 27 Nov 2001 vol 629 cc142-62, 152.
[34] Franziska Boehm and Paul de Hert, *The rights of notification after surveillance is over: ready for recognition?* (Yearbook of the Digital Enlightenment Forum, IOS Press 2012), 19-39.
[35] HL Deb 27 Nov 2001 vol 629 cc183-290, 249.
[36] ibid, 252.
[37] HL Deb 4 Dec vol 629 col. 808-9.
[38] Jim Killock, 'ISPs will break the law if they continue to retain our data' (9 April 2014) <https://www.openrightsgroup.org/blog/2014/are-the-government-and-isps-breaking-the-law-by-continuing-to-retain-our-data> accessed 23 May 2017.
[39] HL Deb 27 Nov 2001 vol 629 cc183-290, 252.
[40] Yves Poullet,'The Fight against Crime and/or the Protection of Privacy: A Thorny Debate!' (2004) International Review of Law Computers and Technology 18:2 251, 252.
[41] ibid.

After the e-PD came into force, nine out of fifteen states planned or were planning to adopt retention legislation.[42] With the controversial Article 15(1)[43] in mind, Statewatch made a prediction that '[o]nce the fundamental principles in the existing 1997 Directive on privacy and telecommunications are cast aside they will never be reinstated.'[44] Tony Bunyan of Statewatch commented that:

> EU governments claimed that changes to the 1997 EC Directive on privacy in telecommunications to allow for data retention and access by the law enforcement agencies would not be binding on Members States - each national parliament would have to decide. Now we know that all along they were intending to make it binding, "compulsory", across Europe.[45]

2.5 Data Retention across Europe and the beginning of the Data Retention Directive

Within the same year of the coming into force of the e-PD, Belgium proposed a (binding) Draft Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions[46] which was leaked to Statewatch.[47] The Decision appeared to speak on behalf of law enforcement *and* service providers across the EU without actually having their opinions referred to (author's emphasis). The Commission noted that *only* an approach that brings together the expertise and capacities of government, industry, data protection supervisory authorities and users will succeed in meeting such goals (author's emphasis).[48] Not only did Statewatch[49] and Privacy International[50] highlight legal flaws of the Draft Framework Decision, but industry also highlighted that data preservation[51] i.e. targeted storage on specified end users should be favoured over data retention.[52] Statewatch noted that

---

[42] Statewatch, 'Majority of governments introducing data retention of communications' <http://www.statewatch.org/news/2003/jan/12eudatret.htm> accessed 23 May 2017.
[43] Daniel B. Garrie and Rebecca Wong, 'Privacy in electronic communications: the regulation of VoIP in the EU and the United States' (2009) C.T.L.R. 15:6 139, 144.
[44] Statewatch, 'EU: Final decision on surveillance of communications European Commission sells-out, European Parliament vote due in May' (January-February 2002) vol 12 no 1, <http://www.statewatch.org/news/2002/may/05Asurv.htm> accessed 25 May 2017.
[45] Statewatch, 'Surveillance of communications: data retention to be "compulsory" for 12-24months' (2002) < http://www.statewatch.org/news/2002/aug/analy11.pdf> accessed 25 May 2017, p1.
[46] Belgium's Draft Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions (2002) <http://www.statewatch.org/news/2002/aug/05datafd.htm> accessed 25 May 2017.
[47] Statewatch, 'Surveillance of communications EU: data retention to be "compulsory" for 12-24 months- draft Framework Decision leaked to Statewatch' (23 August 2002) <http://www.statewatch.org/news/2002/aug/05datafd1.htm> accessed 25 May 2017.
[48] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of Regions: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM/2000/0890 final <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52000DC0890> accessed 25 May 2017, para 48.
[49] Statewatch, (n42).
[50] Privacy International, 'Memorandum of Laws concerning the Legality of Data Retention with regard to the Rights guaranteed by the European Convention on Human Rights' (10 October 2003) <http://www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf> accessed 25 May 2017.
[51] Caspar Bowden, 'Digital Surveillance, Chapter Five Part I' (28 April 2013) <https://www.openrightsgroup.org/ourwork/reports/digital-surveillance/chapter-five-part-I> accessed 25 May 2017.
[52] Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes (4 June 2003) <http://www.statewatch.org/news/2003/jun/CommonIndustryPositionondataretention.pdf> accessed 25 May 2017.

this 'shows that the EU governments always intended to introduce an EC law to bind all member states to adopt data retention.'[53]

Despite the failure of Belgium's Draft Framework Decision, there was another attempt on 28 April 2004 proposed by, the UK, France, Ireland, and Sweden.[54] As Rauhofer notes, due to the general failure of Part 11 of the ATCSA 2001, the UK sought an alternative way to achieve its aim, by focussing on a harmonised approach on the issues of data retention by taking steps to convince other EU Member States to introduce minimum data retention periods.[55]This Draft Framework Decision highlighted the lack of harmonisation between Member States on data retention.[56] However, Cooper and Blaney explained that the date chosen (28 April 2004) by the four governments to table their proposal was deliberately done to marginalise the powers of the Commission and Parliament in the deliberative process as on 1 May 2004, Member States lost their right of initiative and the Commission and EP had gained a 'co-decision procedure' for Third Pillar initiatives with First Pillar ramifications.[57] Not only was this Draft Framework Decision critiqued by Cooper and Blaney, but Statewatch noted the 'grave gaps in civil liberties protection remained' and that it was *worse* than the proposal by Belgium due to its breadth and depth such as extending the retention period (author's emphasis).[58] The Council of Bars and Law Societies of Europe (CCBE)[59] raised concerns about the Draft Framework Decision as although they supported the fight against crime a terrorism, they were worried by the growing initiatives taken at the European level which, under cover of the fight against terrorism, were serious infringements to fundamental freedoms and rights.[60]

The Legal Services for the Council of the EU noted the dubious legality of the Draft Framework Decision,[61] which was withheld from the public and Members of the EP.[62] The EP's Committee on Civil Liberties, Justice and Home Affairs (LIBE) rejected the Draft Framework Decision noting that any such power should be compatible with Article 8 of the ECHR, which

---

[53] Statewatch, (n45), p3.
[54] Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offence including terrorism, Council doc. 8958/04, Brussels, 28 April 2004 <http://www.europarl.europa.eu/RegData/docs_autres_institutions/conseil/2004/08958/CONS_CONS(2004)08958_EN.doc> accessed 25 May 2017.
[55] Judith Rauhofer, (n17), 333.
[56] Draft Framework Decision, (n54), para 8.
[57] Daniel Cooper and Robin Blaney, 'E.U. Data Retention Proposals in the Headlines' (July 2005) <http://www.cov.com/files/Publication/47c9b539-a648-4028-8cea-bd226afe5f09/Presentation/PublicationAttachment/0ed397fe-42fe-4b03-be45-c03607e6f080/oid33931.pdf> accessed 25 May 2017.
[58] Statewatch, 'EU/Surveillance of telecommunications: Data retention comes to roost - telephone and internet privacy to be abolished' (2004) <http://www.statewatch.org/news/2004/apr/21dataretention.htm> accessed 25 May 2017.
[59] The Council of Bars and Law Societies of Europe, 'Comments on the Draft Framework Decision On the Retention of Data' (February 2005) <http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/lobbying_paper_data_1_1182260611.pdf> accessed 25 May 2017. The CCBE represents through its member bars and law societies more than 700,000 lawyers.
[60] ibid, p2.
[61] Opinion of the Legal Service, 'Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism' (5 April 2005) <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207688%202005%20INIT> accessed 25 May 2017.
[62] Chris Jones and Ben Hayes, (n3), p8.

it was not for lack of legality, necessity and proportionality.[63] Importantly the EP noted that the ECtHR:

> [H]as stressed that the contracting states do not have unlimited discretion to subject individuals within their territory to clandestine surveillance. *Given that corresponding powers, conferred on the ground that the intention is to defend democracy, threaten to undermine or destroy democracy*, the Court stresses that *contracting states are not allowed to adopt any measure they deem appropriate in order to combat espionage or terrorism* (author's emphasis).[64]

However, during the rejection of the Draft Framework Decision and the proposal for a Directive, the 7/7 bombings in London had occurred.[65] Just as the 9/11 attacks, this was used a fresh justification for data retention at the EU level.[66] This was despite the then UK Prime Minister, Tony Blair noting that 'all the surveillance in the world' could not have prevented those attacks.[67] As Roger Clarke has noted:

> [M]ost critical driver of change, however, has been the dominance of national security extremism since the 2001 terrorist attacks in the USA, and the preparedness of parliaments in many countries to grant law enforcement agencies any request that they can somehow link to the idea of counter-terrorism.[68]

The UK had used its Presidency of the European Council (Council)[69] to essentially give the EP less than two months' preparation (one year less than for the e-PD) of a final committee report.[70] In addition to this, the EP had to utilise the unduly hasty 'first reading only' procedure which was criticised by many as an attempt on part of the Council and the UK Presidency to 'prevent an in-depth investigation of the actual need for mandatory data retention.'[71] Furthermore, it was reported that then Home Secretary, Charles Clarke (who as noted above apparently did not favour data retention) was reported to have told Members of the EP (MEPs) to agree on proposals or 'he would make sure the EP would no longer have a say on any justice and home affairs matter.'[72] Clarke also noted that if an agreement could not be reached, the prior Framework Decision was still on the table.[73] It was further noted that the UK sought to

---

[63] European Parliament Committee on Civil Liberties, Justice and Home Affairs, 'Report on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism', A6-0174/2005 (31 May 2005) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A6-2005-0174+0+DOC+XML+V0//EN&language=bg> and <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0174+0+DOC+PDF+V0//EN> accessed 26 May 2017.

[64] ibid, fn7 and fn2 respectively.

[65] Chris Jones and Ben Hayes, (n3), p9.

[66] ibid.

[67] Simone Davies, 'Unlawful, unworkable, unnecessary' *The Guardian* (London, 13 July 2005) <https://www.theguardian.com/world/2005/jul/13/humanrights.july7> accessed 30 May 2017.

[68] Roger Clarke, 'Data retention as mass surveillance: the need for an evaluative framework' (2015) International Data Privacy Law 5:2 121, 122.

[69] Chris Jones and Ben Hayes, (n3), p9.

[70] Judith Rauhofer, (n17), 336, fn41.

[71] ibid, 336.

[72] Chris Jones and Ben Hayes, (n3), p9.

[73] Charles Clarke, 'Letter Jean Marie Cavada' (17 October 2005) <http://www.statewatch.org/news/2005/oct/data-ret-clarke-to-cavada-17-10-05.pdf> accessed 29 May 2017.

achieve data retention harmonisation before the end of its Presidency, considering that next in line was Austria, who were firmly against data retention.[74]

The EP had instructed Alexander Alvaro MEP of the LIBE to prepare a report on the proposed Directive, this included a list of compromises but some key changes.[75] When attempts to reach an agreement with the LIBE, the UK used it Presidency to directly target leaders of the two biggest political groups within the EP in a private meeting, making no concessions, yet declaring it a 'compromise.'[76] The DRD came into force on the 3 May 2006 which sought to harmonise data retention across the EU by placing retention obligations on publicly available electronic communications services or public communications networks for harmonisation of telecoms rules law enforcement purposes.[77] This was so despite the pleas from Privacy International (PI), the European Digital Rights Initiative (EDRi), 90 NGOs and 80 telecommunications service providers to MEPs.[78] In the UK, this was subsequently followed by the Data Retention (EC Directive) Regulations 2007[79] and 2009.[80]

2.6 Data Retention at the EU level

(a) Two Opposing Views

There were two contrasting views of the legality of the DRD, that of Francesca Bignami, and Mariuca Morariu. Bignami argued that the DRD was an accessible, detailed and democratically enacted law, continuing that *any* rule (Chapter 7 will highlight this to be incorrect) that is detailed and available to the public satisfies the requirements of the ECHR (author's emphasis).[81] It was further maintained that a two-year retention period was proportionate.[82] Whereas Morariu argued that the DRD raised several controversies such as lock of correlation between aim and objective, lack of definition of serious crime etc and failed to clearly justify its necessity.[83]

(b) Legal Challenges

The first legal challenge to the DRD, was an unsuccessful challenge to its legal basis (i.e. whether it should have been pursued under First (Single Market) or Third Pillar (policing)),[84] with the result being the former. This meant the only way now was to challenge the law itself, which ultimately occurred before the CJEU. Prior to this, however, data retention was met with challenges at a domestic level, with 'Bulgaria's Supreme Administrative Court, the Romanian,

---

[74] Judith Rauhofer, (n17), 336.
[75] ibid, 336-7.
[76] ibid, 338.
[77] Matthew White, (n2), 1.
[78] Chris Jones and Ben Hayes, (n3), p9; Executive Summary of Privacy International and EDRi, 'Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention', (15 September 2004), <http://www.statewatch.org/news/2004/sep/data-retention.htm> accessed 29 May 2017, section 3; Matthew White, (n2), 2.
[79] SI. 2199.
[80] SI. 859
[81] Francesca E. Bignami, 'Privacy and Law Enforcement in the European Union: the Data Retention Directive' (2007) Chicago Journal of International Law 8 233, 249-250.
[82] ibid, 251.
[83] Mariuca Morariu, 'How Secure is to Remain Private? On the Controversies of the European Data Retention Directive' Amsterdam Social Science 1:2 46, 54-9.
[84] Case C-301/06 *Ireland v Parliament and Council* [2009] ECR I-00593, [83-84] and [92-94].

German Federal, Czech Republic Constitutional Courts and the Supreme Court of Cyprus all declaring national implementation of the DRD either invalid or unconstitutional (in some or all regards) and incompatible with Article 8 ECHR.'[85]

Digital Rights Ireland (DRI) brought the first litigation to challenge domestic and European data retention laws on fundamental rights grounds.[86] Before the High Court of Ireland (HCI),[87] DRI amongst others things sought for the HCI to request a preliminary reference to the CJEU on the validity of the DRD under the CFR.[88] The HCI subsequently granted the motion of a preliminary reference to the CJEU under Article 267 of the Treaty of the Functioning of the EU (TFEU).[89] Similarly, the Austrian Constitutional Court[90] sought a preliminary reference on similar grounds, to which the CJEU joined the cases.[91]

(c) A Quest for the Necessity of the DRD

On 9 July 2013, judges of the CJEU's Grand Chamber asked for proof of the necessity and efficiency of the DRD.[92] Despite the lack of statistical evidence from representatives of the Member States, Commission, Council, EP still asked the CJEU to reject the complaints by DRI and others.[93] Only the Austrian government were able to provide the most extensive statistics on *use* of communications data which involved no cases of terrorism (author's emphasis).[94] The UK representative maintained that there was no 'scientific data' to underpin the need of data retention which raised the question of what data the DRD had been therefore based upon.[95] This lack of evidence of *assumed* necessity (from the Commission)[96] was consistent with the findings of the WP29 and the European Data Protection Supervisors (EDPS) (author's emphasis).[97] Moreover, Chris Jones and Ben Hayes note that the plural of the Commission's anecdotes is not 'data' and:

> [E]ven to the extent that case studies can be seen to objectively demonstrate the Directive's effectiveness, it does not necessarily follow that they justify the Directive's

[85] Matthew White, (n2), 2.
[86] T.J. McIntyre, 'Data retention in Ireland: Privacy, policy and proportionality' (2008) Computer Law and Security Report 24:4 326.
[87] *Digital Rights Ireland Ltd -v- Minister for Communication & Ors* [2010] IEHC 221.
[88] ibid, [14-viii].
[89] ibid, [115-iii].
[90] Austrian Constitutional Court, Decision of 28 November 2012, G47/12, G59/12, G62,70,21/12.
[91] Eleni Kosta, 'The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection' (2013) SCRIPTed 10:3 339, 359.
[92] Monika Ermert, 'EU Data retention might not be proportional to risks' (9 July 2013) <https://policyreview.info/articles/news/eu-data-retention-might-not-be-proportional-risks/170> accessed 4 June 2017.
[93] ibid.
[94] ibid.
[95] ibid.
[96] Commission, 'Report from the Commission to the Council and the European Parliament Evaluation report on the Data Retention Directive (Directive 2006/24/EC)' (18 April 2011) COM(2011) 225 final.; European Commission, 'Evidence for necessity of data retention in the EU' (March 2013) <http://www.statewatch.org/news/2013/aug/eu-com-mand-ret-briefing.pdf> accessed 6 June 2017.
[97] Article 29 Working Party, 'European Data Protection Authorities find current implementation of data retention directive unlawful' (14 July 2010) <http://ec.europa.eu/justice/policies/privacy/news/docs/pr_14_07_10_en.pdf> accessed 5 June 2017; Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC) (2011) <http://www.statewatch.org/news/2011/may/edps-opinion-eu-mand-ret-opinion.pdf> accessed 5 June 2017.

scope, application, or absence of *protection for* due process and *fundamental rights* (author's emphasis).[98]

(d) Opinion of Advocate General Cruz Villalón in Digital Rights Ireland

In *Digital Rights Ireland*,[99] Advocate General (AG) Cruz Villalón sought, amongst other things, to determine whether the DRD was 'provided for by law' within the meaning of Article 52(1) of the CFR, and whether it satisfied proportionality within the meaning of Article 52(1).[100] Article 52(1) provides that a limitation of rights contained in the CFR must be provided by law, proportionate in which limitations necessary and genuinely meets objectives of general interest. AG Cruz Villalón proceeded to consider the DRD in light of Article 7 (privacy) and 8 (data protection) CFR,[101] but ultimately considered the DRD in light of Article 7 only[102] because the latter was of secondary importance.[103] AG Cruz Villalón concluded that the DRD as a whole is incompatible with Article 52(1),[104] but this was due to primary focus being on *access* and *use* of data, not its retention (author's emphasis).[105]

(e) Judgment of the CJEU in Digital Rights Ireland

Unlike AG Cruz Villalón, the CJEU ruled that data retention raises questions of not only Article 7 and 8, but also 11 (freedom of expression) CFR.[106] The CJEU, however, proceeded on considering the DRD in light of Articles 7 and 8 only.[107] The CJEU criticised the DRD for practically interfering with fundamental rights of the entire EU population without distinctions, exceptions (professional secrecy), relationships between data retained and the aim pursued (time, geography, persons and serious crime), not laying down substantive and procedural conditions relating to access and subsequent use which was not based on objective criteria, and which above all was not dependent on prior judicial authorisation.[108] The CJEU ruled that the EU legislature exceeded its limits imposed by compliance of proportionality in light of Article 7, 8 and 52(1) CFR,[109] and therefore ruled the DRD as invalid.[110]

(f) The Aftermath of Digital Rights Ireland

[98] Chris Jones and Ben Hayes, (n3), p20.
[99] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] ECR I-845, Opinion of Cruz Villalón.
[100] ibid, [2].
[101] ibid, [54].
[102] ibid, [67].
[103] ibid, [66].
[104] ibid, [131].
[105] ibid, [120-9].
[106] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECR I-238 [25].
[107] ibid, [31].
[108] ibid, [56-68].
[109] ibid, [69].
[110] ibid, [73].

The CJEU's ruling has been regarded as ground-breaking,[111]a milestone,[112] a significant step in developing fundamental rights protection[113] (even in the national security context)[114] and a landmark[115] ruling in that it:

1. Imposed a new level of responsibility on the EU legislator to protect fundamental rights;
2. Subjected EU legislation to a novel strict judicial scrutiny test;
3. Declared invalid EU law for violation of fundamental rights; and
4. Composed substantive instructions for law makers at the EU and Member State level to guarantee suitable protection for privacy and data protection.[116]

The CJEU's position is regarded as closing ranks with the ECtHR jurisprudence by treating collection and use of data as two separate interferences with privacy and data protection.[117] McIntyre argues that it in fact extends protection beyond the ECtHR jurisprudence in that it relied on *ex post facto* controls and takes a step further with regards to need for prior judicial control.[118] However, it has also been argued that this merely reflects already (but not often cited) existing ECtHR jurisprudence.[119] It has also been regarded as putting an end to mass surveillance and comes to the same conclusion as AG Cruz Villalón, but for different reasons.[120] The invalidation of the DRD also meant that it was invalid from the date it came into force.[121]

(g) National Responses to Digital Rights Ireland

Niklas Vainio and Samuli Miettinen noted that there were two interpretations of *Digital Rights Ireland*, permissive and strict.[122] The permissive approach does not take issue with blanket retention in and of itself, but the lack of accompanying safeguards[123] as 'some form of

[111] Emily Barabas, 'European Court of Justice: EU Data Retention Directive Infringes on Human Rights' (April 10 2014) <https://cdt.org/blog/european-court-of-justice-eu-data-retention-directive-infringes-on-human-rights/> accessed 12 June 2017.
[112] Federico Fabbrini, 'Human Rights in the Digital Age The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.' (2015) Harvard Human Rights Journal 28 65, 67.
[113] Judith Rauhofer and Daithí Mac Síthigh, 'The Data Retention Directive Never Existed' (2014) SCRIPTed 11:1 118; EDPS, 'Press Statement: The CJEU rules that Data Retention Directive is invalid' (8 April 2014) <https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2014-08_press_statement_drd_en.pdf> accessed 12 June 2017.
[114] Federico Fabbrini, (n112), 84.
[115] Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) European Law Review 39:6 835, 844; Nora Ni Loideain, 'EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era' (2015) Media and Communication 3:2 53, 54.
[116] Marie-Pierre Granger and Kristina Irion, (n115), 849.
[117] ibid, 847.
[118] T.J. McIntyre, 'Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective' in Martin Scheinin, Helle Krunke, and Marina Aksenova (eds) *Judges as Guardians of Constitutionalism and Human Rights* (Edward Elgar, 2015).
[119] Matthew White, (n2), 5-6.
[120] Steve Peers, 'The data retention judgment: The CJEU prohibits mass surveillance' (8 April 2014) <https://eulawanalysis.blogspot.co.uk/2014/04/the-data-retention-judgment-cjeu.html> accessed 13 June 2017.
[121] Judith Rauhofer and Daithí Mac Síthigh, (n113).
[122] Niklas Vainio and Samuli Miettinen, 'Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States' (2015) International Journal of Law and Information Technology 23:3 290, 299.
[123] ibid, 299-300.

mandatory data retention in order to combat serious crime and terrorism might indeed be compatible with the'[124] CFR. The strict approach entails that blanket indiscriminate data retention is now forbidden[125] as Martin Husovec notes forbidding this 'seems to be an indispensable precondition' given that the following paragraph suggests how to proportionally limit such retention.[126]

The Austrian Constitutional Court (ACC)[127] and Bulgarian Constitutional Court (BCC)[128] both ruled national data retention laws as unconstitutional. As did the Romanian Constitutional Court (RCC).[129] Netherlands's District Court of The Hague (DCH) also ruled that national measures were invalid for going too far, violating freedom of expression and lacked evidence of necessity.[130]

(h) The UK's response to Digital Rights Ireland

For three months, the UK did nothing,[131] then suddenly fast-tracked[132] 'emergency legislation,' the Data Retention and Investigatory Powers Act 2014 (DRIPA 2014) which was adopted within three days.[133] Niklas Vainio and Samuli Miettinen were unconvinced of the UK Government's position that DRIPA 2014 satisfied many of the requirements of *Digital Rights Ireland* as the differences between DRIPA 2014 and the DRR were 'minimal.'[134] A challenge against DRIPA 2014, brought by David Davis MP, Tom Watson MP and others was soon to follow on the grounds of Article 8 ECHR and Article 7 and 8 CFR.[135]

The English and Welsh High Court (HC) ruled that s.1 of DRIPA 2014 was inconsistent with EU law for failing provide clear and precise rules on access and use of communications data in relation to precisely defined serious crimes and not having prior independent/judicial authorisation for said access.[136] The English and Welsh Court of Appeal (CoA) took a radically different approach[137] to the HC, but sought clarification from the CJEU on whether its ruling in *Digital Rights Ireland* were meant to be treated as mandatory requirements (clear and

[124] Coen van Gulijk *et al*, 'SURVEILLE Paper Assessing Surveillance in the Context of Preventing a Terrorist Act' (29 May 2017) <https://www.justsecurity.org/wp-content/uploads/2014/10/SURVEILLE-Paper-on-a-Terrorism-Prevention.pdf> accessed 14 June 2017, p43.
[125] Niklas Vainio and Samuli Miettinen, (n122), 300.
[126] Martin Husovec, 'First European Constitutional Court Suspends Data Retention after the Decision of the Court of Justice of EU' (29 April 2014) <https://cyberlaw.stanford.edu/blog/2014/04/first-european-constitutional-court-suspends-data-retention-after-decision-court> accessed 14 June 2017.
[127] Decision G 47/2012-49, G 59/2012-38, G 62/2012-46, G 70/2012-40, G 71/2012-36 27 June 2014, [3].
[128] Bulgaria Constitutional Court, Decision no. 8/2014, 12 March 2015.
[129] Romania Constitutional Court, Decision no. 653, 8 July 2014, [60-1].
[130] Decision of the District Court of The Hague, Case Number C/09/480009 KG ZA 14/1575, 11 March 2015, [2.2].
[131] Open Rights Group, 'Briefing to MPs on Data Retention Legislation' (9 July 2014) <https://www.openrightsgroup.org/ourwork/reports/briefing-to-mps-on-data-retention-legislation> accessed 15 June 2016.
[132] Matthew White, (n2), 7.
[133] Niklas Vainio and Samuli Miettinen, (n122), 304.
[134] ibid, 305.
[135] ibid; Matthew White, (n2), 7.
[136] *Davis & Ors, R (on the application of) v Secretary of State for the Home Department & Ors* [2015] EWHC 2092, [114].
[137] David Anderson, 'Davis/Watson appeal' (20 November 2015) <https://terrorismlegislationreviewer.independent.gov.uk/daviswatson-appeal/> accessed 18 June 2017.

precise, accessible rules, judicial control of access to communications data etc) by Member States.[138]

(i) Preliminary References

Alongside the CoA's preliminary reference, the Stockholm Administrative Court of Appeals (SACoA) among other things, asked the CJEU whether a general obligation to retain communications data was compatible with Article 15(1) of the e-PD taking account of Articles 7, 8 and 15(1) of the CFR.[139] The President of the CJEU decided to join both references.[140]

(j) Opinion of A-G Saugmandsgaard Øe in Tele2 and Watson

AG Saugmandsgaard Øe in *Tele2 and Watson* noted that Article 15(1) gave Member States a choice[141] and Member States can avail themselves of the possibility subject to the conditions laid out in Article 15(1) itself i.e. general principles of Union law, the CFR and *Digital Rights Ireland*.[142] AG Saugmandsgaard Øe also maintained that the CFR is applicable to national measures of data retention, but not access of police and judicial authorities.[143]AG Saugmandsgaard Øe maintained that *each* of the safeguards mentioned by the CJEU in *Digital Rights Ireland* must be regarded as mandatory.[144] AG Saugmandsgaard Øe concluded that Member States should not be precluded from creating general data retention obligations if such laws are:

1. Accessible, foreseeable and adequately protects against arbitrary interference;
2. Respects the essence of Article 7 and 8 CFR;
3. Strictly necessary i.e. the only measure possible to achieve objective;
4. Accompanied by all the safeguards mentioned in *Digital Rights Ireland*; and
5. Must be proportionate.[145]

(k) The CJEU's Judgment in Tele2 and Watson

Unlike AG Saugmandsgaard Øe, the CJEU held that retention[146] *and* access[147] to communications data fell within the scope of the e-PD (author's emphasis). Furthermore, the CJEU held that data retention not only raises questions of compatibility with Article 7 and 8 CFR, but also Article 11 CFR (freedom of expression),[148] and thus must be taken into account when interpreting Article 15(1) of the e-PD.[149] The CJEU ruled that national laws that implement a general indiscriminate power to retain exceeds the limits of what constitutes what

[138] *Secretary of State for the Home Department v Davis MP & Ors* [2015] EWCA Civ 1185, [118].
[139] Request for a preliminary ruling from the Kammarrätten i Stockholm (Sweden) lodged on 4 May 2015 — *Tele2 Sverige AB v Post- och telestyrelsen* (Case C-203/15).
[140] Case C‑698/15 Order of the President of the Court (Expedited procedure), 1 February 2016.
[141] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-572, Opinion of Saugmandsgaard Øe, [106].
[142] ibid, [116].
[143] ibid, [122-3].
[144] ibid, [226], [244].
[145] ibid, [263].
[146] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-970, [73-5].
[147] ibid, [76-80].
[148] ibid, [92].
[149] ibid, [93]

is strictly necessary in democratic society as required by Article 15(1) as required by Articles 7, 8, 11 and 52(1) CFR.[150]

The CJEU echoed the view of AG Saugmandsgaard Øe in the rules governing access to communications data *must be legally binding* (author's emphasis).[151] The CJEU further elaborated laws governing access must lay down substantive and procedural conditions.[152] The CJEU also favoured notification when it would no longer jeopardise investigations,[153] and to guarantee security and data protection, all data must be retained within the EU, subject to irreversible destruction at the end of the retention period.[154]

(l) Initial Reaction to Tele2 and Watson, and the UK's response

Initial reactions to the CJEU's judgment in *Tele2 and Watson* were positive, many regarding it as a blow to the UK data retention surveillance regime.[155] The Legal Services of the Council acknowledged that 'a general and indiscriminate retention obligation for crime prevention and other security reasons would no more be possible at national level than it is at EU level.'[156] On 30 November 2017, the Home Office responded with a consultation seeking to amend certain provisions of the IPA 2016 (including that which concerns data retention) to comply with *Tele2 and Watson*.[157] These potential amendments will be considered separately (as they are not yet law) for their compatibility with the ECHR in Chapter 7.

In *Tom Watson and Others v Secretary of State for the Home Department*[158] the CoA were asked to determine the legality of DRIPA 2014 in light of *Tele2 and Watson*.[159] Despite ruling that DRIPA 2014 was inconsistent with EU law for not limiting the purposes of retention to fighting serious crime and access to communications data was not based on prior review by a court or administrative body,[160] the CoA declined to grant declaratory relief that it contained no limitations.[161] The three reasons were that:

---

[150] ibid, [107].
[151] ibid, [117].
[152] ibid, [118].
[153] ibid, [121].
[154] ibid, [122].
[155] Javier Ruiz, 'EU Court slams UK data retention surveillance regime' (21 December 2016) <https://www.openrightsgroup.org/blog/2016/eu-court-slams-uk-data-retention-surveillance-regime> accessed 21 June 2017; Julia Fioretti, 'EU court says mass data retention illegal' *Reuters* (London, 21 December 2016) <http://uk.reuters.com/article/uk-eu-court-privacy-idUKKBN14A0YD> accessed 21 June 2017; Owen Bowcott, 'EU's highest court delivers blow to UK snooper's charter' *The Guardian* (London, 21 December 2016) <https://www.theguardian.com/law/2016/dec/21/eus-highest-court-delivers-blow-to-uk-snoopers-charter> accessed 21 June 2017; Nicole Kobe, 'Blow for Snoopers Charter as EU court bans mass data collection' *ITPro* (21 December 2016) <http://www.itpro.co.uk/public-sector/snoopers-charter/27819/blow-for-snoopers-charter-as-eu-court-bans-mass-data-collection> accessed 21 June 2017; Liberty, 'Government IS breaking the law by collecting everyone's internet and call data and accessing it with no independent sign-off and no suspicion of serious crime' (21 December 2016) <https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/government-breaking-law-collecting-everyones-internet-and-call> accessed 21 June 2017.
[156] Legal Services letter to Permanent Representatives Committee, Brussels, 1 February 2017 (OR. en) 5884/17, para 14; See also Anna Biselli, 'EU discusses future of data retention: "Indiscriminate retention no longer possible"' (31 May 2017) <https://edri.org/eu-discusses-future-of-data-retention-indiscriminate-retention-no-longer-possible/> accessed 22 June 2017.
[157] Home Office, 'Open consultation Investigatory Powers Act 2016' (30 November 2017) <https://www.gov.uk/government/consultations/investigatory-powers-act-2016> accessed 15 January 2018.
[158] *Tom Watson and Others v Secretary of State for the Home Department* [2018] EWCA Civ 70.
[159] ibid, [7].
[160] ibid, [27].
[161] ibid, [22-24].

I. It was not argued that DRIPA 2014 was unlawful for failing to provide direct or indirect links between data retained of an identifiable public and serious crime.
II. The CJEU's judgment as in response and applied to Swedish law and therefore not directly applicable to DRIPA 2014; and
III. The HC would be dealing with such matter later that year.

This position is problematic due to it relying on the CJEU's judgment only applying to Swedish law, when it in fact applies to every EU Member State.[162] Moreover, DRIPA 2014 does permit general retention as it allows the possibility to do so, the only difference between Swedish law and DRIPA 2014, is that the former is a 'catch all' and the latter is a 'power that can catch all' to argue otherwise is playing semantics.[163] Instead of addressing the issue, the CoA performed legal gymnastics to avoid answering the question as to whether DRIPA 2014 permitted general data retention.[164]

When the issue came before the HC in *Liberty v Secretary of State for the Home Department and Others*[165] they ruled that the IPA 2016 was incompatible with EU law for the same reasons that DRIPA 2014 was.[166] The HC ruled that s.87(1) of the IPA 2016 did not involve the content of communications,[167] Chapter 3 will disprove this reasoning. The HC also did not consider the ECHR implications of the IPA 2016,[168] nor did they consider that the IPA 2016 permitted general and indiscriminate data retention.[169] This necessitates the importance of this thesis considering data retention through the ECHR, particularly in Chapters 4 and 7.

2.7 Conclusions

This Chapter has briefly demonstrated the politics behind the adoption of data retention measures, particularly in the UK and at an EU level. It has shown that the UK (and not the US) was the main driving force behind data retention harmonisation across the EU through the DRD, something that even the US has never adopted.[170] This has been described as a master class in diplomacy and political manoeuvring[171] but it must also noted that the calls for data retention tend to be at their strongest following an act of terrorism as governments often act in a 'knee-jerk' manner.[172] Simon Davies believed Charles Clarke was hell-bent as an act of political desperation to give the pretence of leadership in Europe.[173] The haste at which the DRD was passed 'left MEPs little time to consider its effect and to organise effective opposition' and those who voted in favour may not have done so on an informed basis.[174]

---

[162] Matthew White, 'Data Retention is still here to stay, for now…' (5 February 2018) <https://eulawanalysis.blogspot.co.uk/2018/02/data-retention-is-still-here-to-stay.html> accessed 1 June 2018.
[163] ibid.
[164] ibid.
[165] *Liberty v Secretary of State for the Home Department and Others* [2018] EWHC 975.
[166] ibid, [186].
[167] ibid, [3].
[168] ibid, [2].
[169] ibid, [120-136].
[170] Chris Jones and Ben Hayes, (n3), p11.
[171] Judith Rauhofer, (n17), 341.
[172] Paul Bernal, 'Terrorism and knee-jerk legislation…' (23 May 2013) <https://paulbernal.wordpress.com/2013/05/23/terrorism-and-knee-jerk-legislation/> accessed 29 May 2017.
[173] Simon Davies, (n67).
[174] Judith Rauhofer, (n17), 342.

Various Member State Courts rejected national implementation of data retention measures which was soon outlawed at an EU level by the CJEU. The CJEU subsequently ruled that general indiscriminate data retention was not permissible in the EU. However, considering that the UK has been a driving force for data retention, with many Member States seeking to follow suit and ignore the CJEU,[175] it is necessary in this thesis to go above and beyond the CJEU and their reasoning, by considering data retention envisaged in Part 4 of the IPA 2016 through the lens of the ECHR. The then EDPS, Peter Hustinx, regarded the DRD as the *most privacy invasive* instrument ever adopted by the EU in terms of scale and the number of people it affects[176] and its compatibility with Article 8 of the ECHR became questionable (author's emphasis).[177] These observations make it crucial to consider in the next Chapter, just how privacy invasive the communications data that can be retained via Part 4 of the IPA 2016.

[175] IT-Pol, 'EU Member States plan to ignore EU Court data retention rulings' (29 November 2017) <https://edri.org/eu-member-states-plan-to-ignore-eu-court-data-retention-rulings/> accessed 15 January 2018.
[176] Peter Hustinx, 'The "moment of truth" for the Data Retention Directive: EDPS demands clear evidence of necessity' (3 December 2010) <http://europa.eu/rapid/press-release_EDPS-10-17_en.htm?locale=en> accessed 25 May 2017.
[177] Judith Rauhofer, (n17), 339; Clive Walker and Yaman Akdeniz, (n16), 179.

Chapter 3: Communications data is just as, if not more intrusive than content

3.1 Introduction

This Chapter focusses specifically on the communications data to be retained and its intrusiveness. In order to achieve this, it first needs to be understood *what* this data is and *where* it comes from. Communications data, also referred to as traffic[1] and metadata[2] is further defined in UK law as Internet Connection Records (ICR) (i.e. website visited), entity Data (i.e. contact details), and events Data (i.e. sending a message/making a call).[3] Though Sophie Stalla-Bourdillon *et al* have argued equating metadata with communications data can be misleading and have the consequence of unduly broadening the scope of telecommunications operators' data retention obligations.[4] This Chapter, will, however, demonstrate that telecommunications operators' data retention obligations *are* unduly broad irrespective of distinctions between communications data and metadata as their analysis took place before the introduction of the Investigatory Powers Act 2016 (IPA 2016).

This Chapter examines the specifics of communications data, relevant communications data, ICR, entity and events Data found within the IPA 2016. Looking into the specifics of these types of data provides an illustration of what it can reveal, and it is against this backdrop that these classes of data will be assessed for their intrusiveness. This Chapter also considers the potential for third party data to be retained and its implications.

The IPA 2016 allows for data to be *generated* for the purposes of retention. It is not clear what this data may be, only that it would include ICRs.[5] This Chapter will highlight that much of the data retention discussion concerns the revealing nature of communications data but little is discussed about the Big Data elephant in the room. This Chapter will give an example of how intrusive the any/all description of data to be retained can be. Finally, this Chapter will briefly note interference becomes more severe based upon whom has access to retained data. This Chapter will therefore conclude that the types of data to be retained (any data *already* in a telecommunications operators' possession, any description of data or capable of obtaining) or generated for retention) puts interference with fundamental rights on the same (if not more) magnitude as content, and thus adversely effects the essence of the right. Such conclusions would mean that the safeguards for content and communications data *should be the same*.

---

[1] Advocate General Saugmandsgaard Øe uses it synonymously in Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-572, [259]; See Executive Summary of Privacy International and EDRi, 'Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention', (15 September 2004), <http://www.statewatch.org/news/2004/sep/data-retention.htm> accessed 29 September 2016.

[2] Big Brother Watch, 'Briefing Note: Why Communications Data (Metadata) Matter' (July 2014) <https://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/07/Communications-Data-Briefing.pdf> accessed 9 October 2017.

[3] *Liberty v Secretary of State for the Home Department and Others* [2018] EWHC 975, [145].

[4] Sophie Stalla-Bourdillon, Evangelia Papadaki and Tim Chown, 'Metadata, Traffic Data, Communications Data, Service Use Information… What Is the Difference? Does the Difference Matter? An Interdisciplinary View from the UK' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move* (Springer 2016), 438.

[5] Section 87(11) of the IPA 2016.

3.2 Communications data and/or Metadata: What is it, and where does it come from?

When discussing data retention, the terminology used is often either communications data or metadata. For the purposes of this thesis, they are one and the same.[6] It is sometimes described as data about data i.e. all other information excluding the content, the where, when, who, how long, and how (of communications).[7] This includes information about the time, duration, and location of a communication as well as the phone numbers or email addresses of the sending and receiving parties.[8] This may also include device information i.e. make/model number.[9] But where does this data come from? Bruce Schneier[10] explains that computers constantly produce data through their input and output, but also as a by-product of everything they do.

Computers continuously document what they are doing i.e. your word processor keeps a record of what you have written, even overwritten versions of what you have written, and only erases them when disk space is needed for something else.[11] Schneier further explains that connecting to the internet only increases the amount of data that is produced, whether it be websites visited, ads clicked on or words typed. Your computer, the sites you visit, the computers in the network all produce data. Your browser sends data to websites about the software you have, when it was installed, the features enabled, to the point where one can be uniquely identified,[12] by for example, unique device IDs (discussed below).

Schneier also notes that data is a by-product of modern technological social interactions, such as the use of social media i.e. Facebook, Twitter, Instagram and Google. These systems do not just transfer data, they also create records of your interactions with others.[13] Schneier continues that mobile phones are constantly producing data about your general location. Use of that phone produces even more data, and with smart phones more still due to the data production of apps and GPS receivers.[14] Newell notes that:

> Metadata is generated whenever a person uses an electronic device (such as a computer, tablet, mobile phone, landline telephone, or even a modern automobile) or an electronic service (such as an email service, social media website, word processing program, or search engine). Often, this results in the creation of considerable amounts of information (metadata).[15]

On the notion of smart phones and social media, Abdulaziz Almehmadi details what he calls the spy in your pocket.[16] Almehmadi notes that smart features on your smartphone are not just tools for collecting personal information for sale, but harvesting information from sensors via

---

[6] Big Brother Watch, (n2).
[7] ibid.
[8] Bryce Clayton Newell, 'The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe' (2014) I/S A Journal of Law and Policy for the Information Society 10:2 481, 488.
[9] ibid.
[10] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W.W. Norton 2016), 15.
[11] ibid.
[12] ibid, 15-16.
[13] ibid, 16.
[14] ibid.
[15] Bryce Clayton Newell, (n8), 488.
[16] Abdulaziz Almehmadi, *The Spy in Your Pocket* (CreateSpace Independent Publishing Platform 2017).

app permissions.[17] Almehmadi gives the example of information collected from ones Global Positioning System (GPS), camera, microphone and contact list.[18] Schneier continues that making purchases creates data, modern cars generate yet more data, from the speed, to how hard pedals are pressed[19]

Schneier came to the conclusion that he had been looking at things backwards, for example, a refrigerator is not a refrigerator with a computer, it's a computer that keeps food cold, your phone is a computer that makes calls, your car is a computer with wheels and an engine.[20] Schneier rightly points out that computers are becoming increasingly embedded into more and more products that are connected to the internet[21] (discussed in greater detail in Chapter 6) which, consequently, will increase the amount of data produced.[22]

3.3 Is communications data just as intrusive as content?

Communications data has often been distinguished from the content of communications. To understand this distinction, it is necessary to understand what content actually means. Content is usually described as what is *within* a message such as the body of an email or conversation over the telephone (author's emphasis).[23] The IPA 2016, s.261(6) defines content as any element of the communication or data logically associated with which reveals anything of what might reasonably considered the meaning of the communication. Section 261(6)(a) and (b), however, considers inferences[24] that can be drawn from communications does not equate to content, neither does systems data[25] as set out in s.263(4).[26] Systems data is described as data which may be used: to identify, or assist in identifying, any person, apparatus, system or service; to identify any event; or to identify the location of any person, event or thing.[27]

This section deals with controversy surrounding the intrusiveness of communications when compared to content.

(a) Not as Intrusive?

UK courts have had a tendency to acknowledge that interception of content is more intrusive than access to communications data.[28] This is also, and not surprisingly, the position of various

[17] ibid, 28.
[18] ibid, 29-38.
[19] Bruce Schneier, (n10), 17.
[20] ibid, 18.
[21] ibid, 18.
[22] ibid, 20.
[23] *Davis & Ors, R (on the application of) v Secretary of State for the Home Department & Ors* [2015] EWHC 2092 (Admin), [13].
[24] Explanatory notes to IPA 2016, para 728.
[25] Which means any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any of the following— (a) a postal service; (b) a telecommunication system (including any apparatus forming part of the system); (c) any telecommunications service provided by means of a telecommunication system; (d) a relevant system (including any apparatus forming part of the system); (e) any service provided by means of a relevant system.
[26] Explanatory notes to IPA 2016, (n24), incorrectly refers to s.264 for the definition of systems data, para 729.
[27] Explanatory notes to IPA 2016, (n24), para 735.
[28] *Davis*, (n23), [81]; *Liberty and Others v Government Communication Head Quarters and Others* [2014] UKIPTrib 13_77-H, 5 December 2014, [34], [111], [114].

law enforcement agencies e.g. the National Crime Agency, police forces etc,[29] and GCHQ.[30] This was also the position of the then Independent Reviewer of Terror Legislation, David Anderson Q.C.[31] The Intelligence and Security Committee (ISC) of the UK Parliament acknowledged that communications data makes it possible to build a richer picture of an individual, but they were of the opinion that it was *significantly* less intrusive than content (author's emphasis).[32] The then Home Secretary, Theresa May MP likened the newly defined ICRs as the modern equivalent of an itemised phone bill.[33] In *Schrems*, the Court of Justice of the European Union (CJEU) maintained that the legislation permitting the public authorities *to have access* on a generalised basis to the *content* of electronic communications must be regarded as compromising the essence of Article 7 (Article 8 ECHR's corresponding right) of the Charter of Fundamental Rights (CFR) (author's emphasis).[34] In contrast, the CJEU in *Digital Rights Ireland* held that data retention does not adversely affect the essence of Article 7 and Article 8 (data protection) *because it does not permit the acquisition of knowledge of the content* of the electronic communications as such (author's emphasis).[35] The essence of the right (which may be similar to the 'very substance of the right')[36] is adopted from the jurisprudence of the European Court of Human Rights (ECtHR).[37] The ECtHR have used the essence of the right for various Convention Rights[38] and therefore, there is no reason why this could not be adopted for the interpretation of Article 8. Though not defined, Hoyano indicates that it may mean that there is an absolute indispensable core to the right which cannot be impaired regardless of the circumstances of any particular instance.[39] The ECtHR in *Uzun v Germany*[40] regarded surveillance via GPS interfered *less* with Article 8 than interception of phone calls. This was used as justification by the Investigatory Powers Tribunal (IPT) in *Liberty and Others v GCHQ and Others* to maintain that interference with communications data *as a whole* was not as serious as interception.[41]

In the USA, there has been an inconsistent approach in regards to communications data. The District Court for the Southern District of New York[42] highlighted that telephone service subscribers maintained no legitimate expectation of privacy in their call data, whereas the District Court for D.C.[43] maintained there is a very significant expectation of privacy.[44]

---

[29] David Anderson, 'A Question of Trust, Report of the Investigatory Powers Review' (June 2015, <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf> accessed 2 March 2016, para 9.30.
[30] ibid, para 10.40(c).
[31] ibid, Annex 2(5), 10.28, 14.53.
[32] Intelligence and Security Committee, *Privacy and Security: A modern and transparent legal framework* (2014, HC 1075) para 143(V).
[33] Theresa May, 'Home Secretary: Publication of draft Investigatory Powers Bill' (4 November 2015) <https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill> accessed 3 April 2017.
[34] Case C‑362/14 *Schrems* [2015] ECR-I 650, [94].
[35] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECR I-238, [39-40]. The High Court took the same approach in *Liberty v Secretary of State for the Home Department and* Others [2018] EWHC 975, [3].
[36] *Geotech Kancev GMBH v Germany* App no. 23646/09 (ECHR, 2 June 2016), [51].
[37] Laura Hoyano, 'What is balanced on the scales of justice? In search of the essence of the right to a fair trial' (2014) Crim. L.R. 1 4, 11.
[38] ibid.
[39] ibid, 15.
[40] *Uzun v Germany* App no. 35623/05 (ECHR, 2 September 2010), [66].
[41] *Liberty and Others*, (n28) [34], [111], [114].
[42] *ACLU v Clapper*, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013).
[43] *Klayman v Obama*, 2013 WL 6571596 (D.D.C. Dec. 16, 2013).
[44] Bryce Clayton Newell, (n8), 510-511.

However, on 22 June 2018, the US Supreme Court ruled that the Government violates the Fourth Amendment (unreasonable search and seizure) by accessing mobile phone location data without a search warrant where there is a legitimate privacy interest.[45] This, however, was only confined to a *type* of communications data, location data, and it is beyond the scope of this thesis to consider what a 'legitimate privacy interest' entails. These contrasting views highlight that there is still a line drawn between communications data, and the content of said communications. Kift and Nissenbaum, however, argue that the National Security Agency's (NSA) position that metadata is non-sensitive data no longer makes sense, nor did it to begin with, because it always created an expectation of privacy.[46]

(b) Just as, if not More Intrusive?

One of the key elements of classifying content as more intrusive than communications data is the assumption that people are more concerned about what they are actually saying, than who they are saying it to. The truth of the matter is that sometimes people care more about the communications data than the content.[47] For example, an email reply with just the text 'lol' reveals very little, but the communications data *associated* with that email can reveal the sender/recipient email address, the date and time it was sent, the subject line, the service used of both sender and recipient, the anti-spam application used and in some instances an approximate location of the sender.[48]

As Schneier suggests, communications data gives us context,[49] and context matters because it gives us meaning.[50] It has been noted that the effect of communications data 'is that a very comprehensive dossier on an individual's private life can be produced (including contacts, where he or she has been, is, or will be going, and his or her interests and habits).'[51] This opinion has also been endorsed by the German Constitutional Court where they believed that 'it cannot automatically be assumed in this connection that recourse to these [sic] data carries fundamentally less weight than the content-based monitoring of telecommunications.'[52] The following press release stated that '[e]ven though the storage does not extend to the contents of the communications, these data may be used to draw *content-related conclusions* that extend into the users' private sphere (author's emphasis).'[53] Saiban and Sykes have also supported this notion by stating that '[a]lthough the content of the data may not be revealed, it will be clear from certain website and email addresses what kind of content *is being viewed* (author's emphasis).'[54] Solove is also of this opinion.[55] This highlights the problematic definition of

[45] *Carpenter v. United States*, No. 16-402, 585 U.S. ____ (2018).
[46] Paula Kift and Helen Nissenbaum, 'Metadata in Context - An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program' (2017) ISJLP 13 333.
[47] Daniel Solove, *Understanding Privacy* (Harvard University Press 2009), 68; Daniel Solove, 'Reconstructing Electronic Surveillance Law' (2004) 72 The George Washington Law Review 1701, 1728.
[48] Guy McDowell, 'What Can You Learn From An Email Header (Metadata)?' (13 August 2013) <http://www.makeuseof.com/tag/what-can-you-learn-from-an-email-header-metadata/> accessed 4 April 2017.
[49] Bruce Schneier, (n10), 26.
[50] Penny Tompkins and James Lawley, 'Context Matters' (5 April 2003) <http://www.cleanlanguage.co.uk/articles/articles/205/1/Context-Matters/Page1.html> accessed 3 April 2017.
[51] Nick Taylor, 'Policing, privacy and proportionality' (2003) European Human Rights Law Review 86, 97.
[52] BVerfG, judgment of the First Senate of 02 March 2010 - 1 BvR 256/08 - Rn. (1-345), [227].
[53] Bundesverfassungsgericht, 'Data retention unconstitutional in its present form' (March 2010) <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html > accessed 4 April 2017.
[54] Jason Saiban and John Sykes, 'UK ANTI-TERRORISM ACT 2001 & ISP'S: A CYBER CHECK-POINT CHARLIE?' (2002) Computer Law & Security Review 18:5 338, 338.
[55] Daniel Solove, Reconstructing Electronic Surveillance Law, (n47), 1726-1728.

content in s.261(6) of IPA 2016 as it essentially proclaims content is meaning, but not *that* kind of meaning that can be gained from the communications data (even if it produces the *same* meaning). The explanatory notes to the IPA 2016 noted that '[w]hile it is possible to draw an inference from the fact a person has contacted another person this is distinct from the content of, for example, the telephone call.'[56] This, distinction however, does not reflect reality as a study by Stanford University demonstrated the type of inferences they could draw from phone metadata.[57]

It is difficult to conclude that such inferences do not detail the meaning of the communication. Moreover, collected internet traffic data has even been regarded by Alberto Escudero-Pascual and Gus Hosein as mildly *more sensitive* than traditional telephone traffic data (author's emphasis).[58] This is why it was unhelpful for the then Home Secretary, Theresa May MP to claim that ICR were equivalent to phone bills as her own evidence submitted to the draft Joint Committee of the Investigatory Powers Bill demonstrated that communications data goes well beyond just billing data.[59] May's statement is contradicted when considering ICRs[60] as a telephone bill can reveal who you've been speaking to, when and for how long, but your internet activity reveals *everything* you do online (author's emphasis).[61]

This is why it has been suggested that interference with communications data at the very least is as *just as serious* as interference with content (author's emphasis).[62] The Royal United Services Institute (RUSI), considered that this might be a possibility.[63] Advocate General (AG) Saugmandsgaard Øe in *Tele2 and Watson* noted that that in the *individual context* a general data retention obligation would facilitate *equally serious interference* as targeted surveillance measures, *including those which intercept the content of communications* (author's emphasis).[64] The Article 29 Data Protection Working Party (WP29) was of the opinion that metadata and content should both have the same high level of protection.[65]

Escudero-Pascual and Hosein have suggested that '[t]raffic data analysis generates *more sensitive profiles of an individual's actions and intentions, arguably more so than*

[56] Explanatory notes to IPA 2016 (n24), para 728.
[57] Jonathan Mayera, Patrick Mutchlera, and John C. Mitchella, 'Evaluating the privacy properties of telephone metadata' (2016) PNAS 113:20 5536, 5540.
[58] Alberto Escudero-Pascual and Gus Hosein, 'Questioning lawful access to traffic data' (2004) Communications of the ACM 47:3 77, 80.
[59] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (February 2016), <http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf> accessed 5 April 2017, Home Office, 515-517.
[60] Paul Bernal, 'A few words on 'Internet Connection Records'' (5 November 2015) <https://paulbernal.wordpress.com/2015/11/05/a-few-words-on-internet-connection-records/> accessed 5 April 2017.
[61] Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill* (2015-16, HL 93, HC 651) 123.
[62] Elisabet Fura and Mark Klamberg, 'The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA' in Josep Casadevall, Egbert Myjer, Michael O'Boyle (eds) *Freedom of Expression – Essays in honour of Nicolas Bratza – President of the European Court of Human Rights* (Wolf Legal Publishers, Oisterwijk 2012), 467.
[63] RUSI, 'A Democratic Licence to Operate' (15 July 2015) <https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf> accessed 3 April 2017, para 1.44-1.46.
[64] Joined Cases C‑203/15 and C‑698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-572, Opinion of Saugmandsgaard Øe, [254].
[65] Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), para 18.

communications content (author's emphasis).'[66] [AG] Saugmandsgaard Øe in *Tele2 and Watson* maintained that risks associated with the access to communications data may be greater than access to the content of communications.[67] As Roberts notes, the interference posed by data retention cannot solely be based on the nature of the data but also whom has access.[68] Paul Bernal notes that gathering of communications data is of a greater intrusion than the examination of content. This is because communications data is structured, making it more suitable for aggregation and analysis. Furthermore, content can be disguised more easily through encryption[69] or using coded language.[70] Examples of how communications data can constitute a greater intrusion than content is now to be provided. Andrew Reed and Michael Kranch demonstrated, even with a HTTPS (encrypted) protected Netflix videos, the videos watched could still be identified using only the TCP/IP headers[71] (which would be classed as relevant communications data).[72] Bernal notes many intimate subjects are often deliberately avoided (to avoid disclosure of sexuality, religion and health information) when writing content, this can be determined by communications data analysis.[73]

This revealing nature is given further weight based on its usefulness in terms of prevention or detection of crime, or the prevention of disorder, or prevention of death or injury or safeguarding national security.[74] The ISC were 'surprised to discover that the primary value to GCHQ of bulk interception was not in reading the actual content of communications, *but in the information associated with those communications* (author's emphasis).'[75] The NSA's General Counsel, Stewart Baker admitted that 'metadata absolutely tells you everything about somebody's life. If you have enough metadata, *you don't really need content* (author's emphasis).'[76] Former director of the NSA and the Central Intelligence Agency (CIA), Michael Hayden agreed with Bakers comments as being 'absolutely correct' because '[w]e kill people based on metadata.'[77] Using metadata from 55 million phone users in Pakistan aids NSA in who to target for drone strikes.[78]

---

[66] Alberto Escudero-Pascual and Gus Hosein, (n58), 82.
[67] Opinion of Saugmandsgaard Øe, (n64), [259].
[68] Andrew Roberts, 'Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications' (2015) MLR 78:3 522, 545.
[69] Paul Bernal, 'Data gathering, surveillance and human rights: recasting the debate,' (2016) Journal of Cyber Policy 1:2 243, 248.
[70] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n59), Paul Bernal, para 3.9, p132.
[71] Andrew Reed and Michael Kranch, 'Identifying HTTPS-Protected Netflix Videos in Real-Time' (March 2017) <http://www.mjkranch.com/docs/CODASPY17_Kranch_Reed_IdentifyingHTTPSNetflix.pdf> accessed 9 April 2017.
[72]Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n59), Brass Horns Communications, p191.
[73] ibid, Paul Bernal, para 3.9, p132.
[74] David Anderson, (n29), para 9.21; Home Office, 'Communications data' (17 March 2015) < https://www.gov.uk/government/collections/communications-data> accessed 3 April 2017; see also Commission of the European Communities, Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, COM (2005) 438 Final September 2005, section 1.2.
[75] Intelligence and Security Committee, (n32), para 80.
[76] Mike Masnik, 'Michael Hayden Gleefully Admits: We Kill People Based On Metadata' *Techdirt* (12 May 2014) <https://www.techdirt.com/articles/20140511/06390427191/michael-%20hayden-gleefully-admits-we-kill-people-based-metadata.shtml> accessed 9 April 2017.
[77] David Cole, 'We Kill People Based on Metadata' *The New York Review of Books* (New York City, 10 May 2014) <http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/> accessed 9 April 2017.
[78] John Naughton, 'Death by drone strike, dished out by algorithm' *The Guardian* (London, 21 February 2016) <https://www.theguardian.com/commentisfree/2016/feb/21/death-from-above-nia-csa-skynet-algorithm-drones-pakistan> accessed 3 June 2018.

Most importantly, the ECtHR in *Big Brother Watch* were not persuaded:

> [T]hat the acquisition of related communications data is necessarily less intrusive than the acquisition of content. For example, the content of an electronic communication might be encrypted and, even if it were decrypted, might not reveal anything of note about the sender or recipient. The related communications data, on the other hand, could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with.[79]

The ECtHR's position echoes arguments made in this subsection, and takes a step further than the CJEU in considering content and communications data as equals. This has important ramifications for appropriate safeguards when communications data is concerned (see Chapter 5). One could argue that the IPT in *Liberty and Others* used the ECtHR's ruling in *Uzun* to make the distinction between communications data and content. However, the:

> The IPT's reasoning was based on the false analogy raised by the Respondent…that because GPS data didn't amount to the required seriousness of that of interception, the same principle applied to communications data. However, in accepting this analogy the IPT made a critical error as location data, derived from GPS isn't the only data that forms part of the broad definition of communications data…Therefore, when the IPT gave weight to Uzun it did so by considering a case of an isolated specific type of data, which cannot be used to justify an argument that interference is less severe whilst ignoring the cumulative total of the different types of communications data.[80]

In further support of the ECtHR's position, it is important to now consider communications data as envisaged in the IPA 2016 and the level of intrusiveness.

3.4 Data by type and intrusiveness

Part 4 of the IPA 2016 concerns the issuing of data retention notices. This part also provides insight into what data can be retained. Section 87(1) of the IPA 2016 allows the Secretary of State to issue retention notices on telecommunication operators to retain 'relevant communications data.' Section 87(4) details that telecommunications operators are not to retain 'third-party' data,[81] but s.87(4)(d) allows this data to be required to be retained if it is used or retained for a lawful purpose. Section 87(11) concerns the retention of ICRs and s.87(9)(b)(i) provides that retention notices can obligate data to be generated for the purposes of retention. It is necessary to break down and discuss relevant communications data, third party data, ICRs, generated data and their intrusiveness separately.

(a) Relevant Communications Data

[79] *Big Brother Watch v UK* App nos. 58170/13, 62322/14 and 24960/15 (ECHR, 13 September 2018), [356].
[80] Matthew White, 'Protection by Judicial Oversight, or an Oversight in Protection?' (2017) Journal of Information Rights, Policy and Practice 2:1 1, 9.
[81] Explanatory notes to IPA 2016, (n24), para 262.

According to s.87(11) of the IPA 2016, relevant communications data includes the sender or recipient (human or not) of a communication, its time, duration, type, mode/pattern or fact of communication, the telecommunications system[82] the communication has been transmitted to, from or through and its location.

These five categories, Graham Smith suggests, at face value appear to go wider than the data types found under the Data Retention and Investigatory Powers Act 2014 (DRIPA 2014) (which implemented the DRD definitions) as amended by the Counter Terrorism and Security Act 2015 (CTSA 2015).[83] Smith notes that the scope of 'relevant communications data' captures communications not just between humans. This, Smith highlights, 'sweeps up not only background interactions that smartphone apps make automatically with their supplier servers, but probably the entire internet of things'[84] (see Chapter 6). Smith continues that 'data such as the 'type, method or pattern' of communication' extend beyond the familiar sender/recipient, time and location.[85] For example, logging onto Facebook via an iPhone using Safari.

Smith highlights that when considering what relevant communications data consists of, there are 14 (with 'identifier' no longer present in the IPA 2016) interlinked definitions that make it up.[86] This includes:

1. Relevant communications data,
2. Telecommunications system,
3. Person,
4. Communications data,
5. Communication,
6. Apparatus,
7. Telecommunications operator,
8. Telecommunications service,
9. Entity data,
10. Events data,
11. Entity,
12. Content of a communication; and,
13. Data.

Telecommunications operator/service/system and apparatus will be dealt with in more detail in Chapter 6 highlighting that what can be retained is dependent on who can be obligated to retain. Although s.87 of the IPA 2016 refers to 'relevant communications data' it is important to note that s.261(5)(a) defines *communications data* as either entity or events data which is or is capable of being held or obtained, by or on behalf of the telecommunications operators. This includes data held by a telecommunications operator or available directly from the network which identifies a person or device on the network, ensures that a communication reaches its

[82] See Chapter 6.
[83] Graham Smith, 'Never mind Internet Connection Records, what about Relevant Communications Data?' (29 November 2015) <http://www.cyberleagle.com/2015/11/never-mind-internet-connection-records.html> accessed 8 April 2017.
[84] ibid.
[85] ibid.
[86] ibid.

intended destination, describes how a person has been using a service or is about the architecture of the telecommunication system itself.[87]

Entity (which is a person or thing)[88] data refers to data about entities or links between them and telecommunications service/systems but according to the explanatory notes does not include information about individual events,[89] this includes phone numbers, service identifiers, physical address, or IP addresses.[90] Section 81(1) of the Regulation of Investigatory Powers Act 2000 (RIPA 2000) defines person (which the IPA 2016 is silent on) as including any organisation and any association or combination of persons. Therefore, entity data can be summarised as data about an individual, any group of individuals or any object. This, therefore, contrary to the explanatory notes, *can* provide information about individual events.

Events data is defined in s.261(4) and can be summarised as identifying and describing events taking place on a telecommunication system or other device which consist of one or more entities engaging in an activity at a specific point, or points, in time and space.[91] The explanatory notes to IPA 2016 gives examples of the fact that 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.[92] The explanatory notes also details that entity data is generally less intrusive than events data without explaining why.[93]

Given that the relevant definitions discussed above recite 'communication' and 'data' frequently, it is important to highlight their definitions also.[94] Communication is defined in s.261(2) as:

a) anything comprising speech, music, sounds, visual images or data of any description, and
b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus.

Data is defined in s.263(1) which includes data which is not electronic data and any information (whether or not electronic). Combining these definitions above will later highlight that the types of data that can be retained under Part 4 is essentially limitless. However, in order to make sense of the relevant communications data issue, some insight can be gleamed from the Home Secretary, who presented evidence to the Joint Committee on the Draft Investigatory Powers Bill gave a table (see Table A) of examples what is considered to be communications data and content.[95] Although not a definitive legal source, it does give some insight into what is considered communications data.

---

[87] Explanatory notes to IPA 2016, (n24), para 723.
[88] Section 261(7) of the IPA 2016.
[89] Explanatory notes to IPA 2016, (n24), para 725.
[90] ibid, para 727.
[91] ibid, para 726.
[92] ibid, para 727.
[93] ibid, para 223.
[94] For an excellent breakdown of definitions, see Graham Smith, 'Relevant Communications Data revisited' (15 March 2016) <http://www.cyberleagle.com/2016/03/relevant-communications-data-revisited.html> accessed 9 April 2017.
[95] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n59), Home Office, p515-517; Similar to the types of data found in the Retention of Communications Data under Part 11: Anti-terrorism,

<table>
<tr><th colspan="3">Communications data</th><th>Content</th></tr>
<tr><td colspan="4">Postal</td></tr>
<tr><td>• Name of a customer of a postal product
• Address of a customer of a postal product
• Phone number of a customer of a postal product
• Email address linked to a customer's account of a postal product</td><td>• Any redirections in place on a customer's account
• Account details used to pay for the service
• The address on a letter or parcel in the postal system</td><td>• Any replacement address put on a letter or parcel to facilitate re-direction
• Billing data for sending mail (e.g. corporate account)</td><td>• The content of a letter or parcel
NB for a postcard the content would be the message on the postcard and picture on the front. The address and other information added to facilitate delivery of the package would be communications data.</td></tr>
<tr><td colspan="4">Mobile Telephony including SMS, MMS, EMS</td></tr>
<tr><td>• Cell mast name
• Cell mast locations
• Cell mast sector
• Network maps
• 2G/3G/4G coverage maps
• Name/address of a customer</td><td>• Email address linked to a customer's account
• Device identifiers linked to a customer's account – e.g. IMSI, IMEI, Mac Address
• Account details used to pay for the service
• Dialled phone number
• Phone number of a customer</td><td>• Dialling phone number
• Time/date/location a phone call was made
• Device identifiers linked to a communication
• Billing data
• A handshake between a phone and a cell mast so the network knows where to route a call</td><td>• The audio of a phone call
• The body of a text message
• An image sent as an MMS</td></tr>
<tr><td colspan="4">Internet access NB – this may additionally include information in relation to internet applications (below) where held by the internet access provider for business purposes</td></tr>
</table>

Crime and Security Act 2001 Voluntary Code of Practice <http://www.opsi.gov.uk/si/si2003/draft/5b.pdf> accessed 17 April 2017.

Broadband	Public Wi-fi	Mobile	
• Routing information • Name of a customer • Address of a customer • Phone number of a customer • Device identifiers linked to a customer's account –e.g. IMSI, IMEI, MAC Address • Email address linked to a customer's account • Account details used to pay for the service • User name • Password • Billing data • RADIUS logs (IP session start/stop) • Destination IP address and port number • The domain url (this is the part such as bbc.co.uk)** • Server Names indicator** • Public source IP address and port number • Time/date/location of an internet communication • Device identifiers linked to a communication • Volumes of data uploaded/downloaded	Instead of the location/address of the broadband router the following data may additionally be captured: • Wi-fi access point name • Wi-fi access point address • Wi-fi access point device identifiers e.g. MAC address • Cover age maps NB – What may appear as a single wi-fi access session to a customer may actually constitute multiple sessions using different wi-fi access points or a number of applications on a device opening separate connections. A session may also use mobile data for some periods where the data in the next column	Instead of the location/address of the broadband router the following data may additionally be captured: • Cell mast name • Cell mast sector • Cell mast locations • Network maps • 2G/3G/4G coverage maps • Device identifiers (e.g. MAC address, IMSI, IMEI) of the device connecting to the mobile internet – e.g. phone, tablet, dongle • Device identifiers (e.g. MAC address) of any other devices using the internet through that connection (some devices can broadcast their signal allowing another device to use their connection). • A handshake between a phone and a cell mast so the network knows where to route a mobile data session • NAT/PAT logs NB – what may appear to a customer to be a single mobile	• The url of a webpage in a browsing session (e.g. www.bbc.co.uk/news/story or news.bbc.co.uk or friend'sname.facebook.com) • The content of the webpages being viewed, including any text, images, audio and videos embedded in the page • The names and content of any files transmitted over a peer to peer connection • Private posts being transmitted to or viewed on a webserver * • A like message being posted on social media * NB – in practice an internet access provider is often unable to distinguish what traffic it is carrying from a source IP to a destination IP.

• Location/address of access point such a broadband router	will be relevant	internet session may be multiple sessions for the same reasons as for public wi-fi access.	
Internet applications (such as Internet Telephony, Internet email)			
• Routing information • Name of a customer • Address of a customer • Phone number of a customer • Email address linked to a customer's account • Time/date/location at logon/logoff/reconnect	• Account details used to pay for the service • User name (or other credentials used to access the service)*** • Password • Billing data	• Email address of the sender or recipient of an email • Caller and callee for voip calls • Source IP address and port number • Message type (e.g. email, IM) • Time/date/location of each internet communication	• The body of an email • The subject line of an email • Any attachments to an email • The audio/ visual of an internet call • The messages comprising a conversation in an internet chat

Table A

(b) Passwords and Usernames

The definition applies to username and passwords associated with Broadband (i.e. BT, Virgin, Talktalk) and what the Home Secretary regards as Internet applications such as Internet telephony (i.e. Skype, Whatsapp) and Internet email (i.e. Gmail, Hotmail etc). It must be noted that Internet applications does not appear to be limited to Internet telephony and Internet email, and this therefore could include web browsing (i.e. Safari, Chrome), peer-to-peer services (i.e. BitTorrent, Utorrent).[96] This can also include media (i.e. Youtube, BBC iPlayer) information search (i.e. Google search, Bing search), communities (i.e. Facebook, Twitter), entertainment (i.e. Playstation Network, X-Box Live, Netflix), e-business (i.e. Amazon, eBay), finance (i.e. Barclays online banking) and other applications.[97] Many of these applications can overlap, but the examples serve to highlight the breadth of coverage.

As Kevin Fu *et al* note

> Passwords are the primary means of authenticating users on the Web today. It is important that any Web site guard the passwords of its users carefully. This is especially

[96] Encyclopaedia 'Internet Applications' <http://www.encyclopedia.com/computing/news-wires-white-papers-and-books/internet-applications> accessed 10 April 2017.
[97] National Institute of Open Schooling 'Internet Applications and Services' <http://oer.nios.ac.in/wiki/index.php/INTERNET_APPLICATION_AND_SERVICES> accessed 10 April 2017.

> important since users, when faced with many Web sites requiring passwords, tend to reuse passwords across sites.[98]

They continue that '[c]ompromise of a password completely compromises a user.'[99] It is this compromising nature which puts passwords and usernames at the most intrusive end of communications data. Some passwords need not be stored for authentication,[100] would they require generation for the purposes of retention via s. 87(9)(b)(i)? If a Broadband provider provides the router, this will contain network/router username and password, which would be classed as communications data. Obtaining a router's username and password can lead to malicious actors pretending to be genuine sites with the aim of stealing username and passwords for other internet applications, such as bank details.[101] Obtaining network username and password can lead to all traffic being intercepted.[102] If any of the traffic is difficult to intercept because of the use of a third party application (which uses encryption), then the username and password for these services (which would fall under Internet applications) could also be used to defeat encryption. Moreover, if the username and password for example, Google Password Manager[103] was compromised, this would reduce the difficulty in gaining access to other Internet applications. This not only demonstrates an example of entity data[104] being more intrusive than events data, but how two types of communications data could compromise essentially anything done online. These two types of data alone would make any argument that content is more intrusive than communications data superfluous because not even the services provided to the consumer can guarantee safety,[105] let alone the Government.[106]

(c) Unique Identifiers and Location Data

---

[98] Kevin Fu, Emil Sit, Kendra Smith, Nick Feamster, 'Dos and Don'ts of Client Authentication on the Web' (2001) <http://static.usenix.org/publications/library/proceedings/sec01/full_papers/fu/fu_html/> accessed 10 April 2017.

[99] ibid.

[100] Leigh Lundin, 'PINs and Passwords, Part 2' (11 August 2013) <http://www.sleuthsayers.org/2013/08/pins-and-passwords-part-2.html> accessed 10 April 2017.

[101] Michael Horowitz, 'Defending your router, and your identity, with a password change' (19 March 2008) <https://www.cnet.com/uk/news/defending-your-router-and-your-identity-with-a-password-change/> accessed 10 April 2017.

[102] Mike Chapple, 'Wireshark tutorial: How to sniff network traffic' *TechTarget* (Newton, Massachusetts, October 2008) <http://searchsecurity.techtarget.com/tip/Wireshark-tutorial-How-to-sniff-network-traffic> accessed 10 April 2017.

[103] Amit Agarwal, 'Access your Passwords from Anywhere with Google Password Manager' (1 February 2016) <https://www.labnol.org/internet/google-passwords-manager/29077/> accessed 10 April 2017; Abdulaziz Almehmadi, (n16), 60-61.

[104] Home Office, 'Communications Data DRAFT Code of Practice' (November 2017) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/663675/November_2017_IPA_Consultation_-_Draft_Communications_Data_Code_of_Pract....pdf> accessed 16 January 2018, para 2.42.

[105] Alfred Ng, Steven Musil, 'Equifax data breach may affect nearly half the US population' *CNet* (7 September 2017) <https://www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population/> accessed 10 October 2017; Andrea Peterson, 'eBay asks 145 million users to change passwords after data breach' *The Washington Post* (Washington, D.C, 21 May 2014) <https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/> accessed 10 October 2017.

[106] BBC, 'Previous cases of missing data' *BBC News* (London, 25 May 2009) <http://news.bbc.co.uk/1/hi/uk/7449927.stm> accessed 10 October 2017.

There are various identifiers for phones alone.[107] Table A also regards device identifiers that are linked to a customer's Broadband/mobile account as communications data. Moreover, this includes the identifiers associated with communications associated with said Broadband/mobile service. Finally, communications data also consists of Wi-Fi access point identifiers, device identifiers when using mobile internet and any devices identifiers of any other devices using the internet through that connection. The Home Secretary's evidence gives an example of such identifier, the Media Access Control (MAC). These are unique hardware numbers for computers.[108] Bluetooth technologies periodically advertise MAC addresses.[109] According to Edward Snowden the NSA has a system that tracks the movements of everyone in a city by monitoring the MAC addresses of their electronic devices,[110] Cunche agrees this is very possible,[111] with traffic and retail store monitoring already happening.[112] Tim Banks argues that 'there is a greater probability of correlation between the owner of the device and the MAC address than there is of an IP address and an individual.'[113] This is possibly because IP addresses can be dynamic i.e. the IP address changes each time there is a new connection to the internet, as noted in Breyer,[114] whereas MAC addresses are not (unless hidden by the device owner).[115] Mapping the movements is also possible through other devices identifiers such as the International Mobile Subscriber Identity (IMSI) and the International Mobile Station Equipment Identity (IMEI) numbers. These are also classed as communications data. IMSI and IMEI numbers are unique mobile device identifiers, in which ISMI catchers[116] can retrofit location monitoring technologies to determine the location of a target within one metre,[117] though they have been argued to not be as effective as once thought.[118]

This leads to the necessary discussion regarding location data/information[119] given that this also falls under communications data. Location data/information is regarded 'as any type of data that places an individual at a particular location at any given point in time, or at a series

---

[107] Christopher Parsons, 'Privacy Tech-Know Blog: Uniquely You: The identifiers on our phones that are used to track us' (8 December 2016) <http://blog.priv.gc.ca/index.php/2016/12/08/privacy-tech-know-blog-uniquely-you-the-identifiers-on-our-phones-that-are-used-to-track-us/> accessed 24 April 2017.

[108] Margaret Rouse, 'MAC address (Media Access Control address)' *TechTarget* <http://searchnetworking.techtarget.com/definition/MAC-address> accessed 10 April 2017; for a more technical definition see Mathieu Cunche, 'I know your MAC address: targeted tracking of individual using Wi-Fi' (2014) Journal of Computer Virology and Hacking Techniques 10:4 <https://hal.inria.fr/hal-00858324/document> accessed 10 April 2017.

[109] Mathieu Cunche, (n108).

[110] James Bamford, 'The Most Wanted Man in the World' *Wired* (San Francisco, California, 13 June 2014) <http://www.wired.com/2014/08/edward-snowden/> accessed 10 April 2017.

[111] Mathieu Cunche, (n108).

[112] ibid.

[113] Tim Banks, 'MAC and IP Addresses: Personal Information?' (24 July 2012) <http://www.privacyanddatasecuritylaw.com/mac-and-ip-addresses-personal-information> accessed 10 April 2017.

[114] Case C‑582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECR I-779, [16].

[115] Chris Hoffman, 'How (and Why) to Change Your MAC Address on Windows, Linux, and Mac' (30 June 2014) <https://www.howtogeek.com/192173/how-and-why-to-change-your-mac-address-on-windows-linux-and-mac/> accessed 11 April 2017.

[116] Christopher Parsons, 'IMSI Catchers in Canada Resources' <https://www.christopher-parsons.com/writings/imsi-catchers-resource-page/> accessed 11 April 2017.

[117] Privacy International, 'Location Monitoring' <https://www.privacyinternational.org/node/74> accessed 11 April 2017.

[118] Kenneth van Rijsbergen, 'The effectiveness of a homemade IMSI catcher build with YateBTS and a BladeRF' (2015) <http://www.delaat.net/rp/2015-2016/p86/report.pdf> accessed 10 October 2017.

[119] Anne S.Y. Cheung, 'Location privacy: The challenges of mobile service devices' (2014) Computer Law and Security Review 30 41, 43 'In this article, the terms 'location data' and 'location information' are used *interchangeably*.'

of locations over time.'[120] This also encompasses 'geo-positioning other than latitude, longitude and altitude, which can be ascertained with varying degrees of precision.'[121] There is another important term, geo-location data, which refers to data generated by electronic devices that can be used to determine the location of the relevant devices and their users.'[122] The WP29 regards that 'the combination of a MAC address of a WiFi access point with its calculated location' should be treated as personal data.[123] Location data is also regarded as personal data for the purposes of Article 4(1) of the Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR)).

In Recommendation AAA, the ISC regards approximate location data to be not as sensitive as communications data plus because the latter includes a more detailed class of information about a person's habits, such as preferences or lifestyle choices and websites visited.[124] However, as Teresa Scassa[125] and Anne Uteck[126] have suggested, location data can be used to create a data picture of movements of identifiable individuals.[127] Rozemarijn van der Hilst would go further than the WP29 and GDPR and argue that location could be considered 'sensitive personal data'[128] or a 'special category of personal data because 'it can reveal information about a person's habits, (future) whereabouts, religion, and can even reveal sexual preference or political views.'[129] This highlights not only that location data can reveal very intimate details, it can be used to make future predictions based on current data possessed.[130] Though the WP29 did acknowledge that:

> A behavioural pattern may also include special categories of data, if it for example reveals visits to hospitals and religious place, presence at political demonstrations or presence at other specific locations revealing data about for example sex life.[131]

Sensitive/special categories of personal data is defined in Article 9(1) of the GDPR as:

---

[120] ibid.
[121] ibid.
[122] ibid.
[123] ARTICLE 29 Data Protection Working Party, 'Opinion 13/2011 on Geolocation services on smart mobile devices' (adopted 16 may 2011) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf> accessed 13 April 2017.
[124] Intelligence and Security Committee, (n32).
[125] Teresa Scassa, 'Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy' (2009) Canadian Journal of Law and Technology 9:2 193.
[126] Anne Uteck, "Ubiquitous Computing and Spatial Privacy" in Ian Kerr *et. al.*, eds., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford: Oxford University Press, 2009), 85.
[127] Anne S.Y. Cheung, (n119), 43; see also Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen and Vincent D. Blondel, ' Unique in the Crowd: The privacy bounds of human mobility' (2013) Scientific Reports 3:1376 1.
[128] Rozemarijn van der Hilst, 'Characteristics and uses of selected detection technologies, including their potential human rights' (30 November 2011) <http://www.detecter.bham.ac.uk/pdfs/17_3_tracking_technologies.doc> accessed 13 April 2017, 2, 33, 38.
[129] ibid, 38.
[130] Daniel Ashbrook and Thad Starner, 'Using GPS to learn significant locations and predict movement across multiple users' (2003) Pers. Ubiquitous Comput. 7:5 275; Marta C. Gonza´lez, Ce´sar A. Hidalgo and Albert-La´szlo´ Baraba´si, 'Understanding individual human mobility patterns' (2008) Nature 453 779; Lars Backstrom, Eric Sun and Cameron Marlow, 'Find Me If You Can: Improving Geographical Prediction with Social and Spatial Proximity' (2008) <http://cameronmarlow.com/media/backstrom-geographical-prediction_0.pdf> accessed 14 April 2017.
[131] ARTICLE 29 Data Protection Working Party, (n123).

> [P]ersonal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation...

The Grand Chamber (GC) of the ECtHR in *S and Marper* highlighted that where ethnic origin can be inferred from data, their retention is 'all the more sensitive and susceptible of affecting the right to private life.'[132] Abdulaziz Almehmadi details a real-life example of how Google Maps could generate a pattern of lifestyle, who one is and how time is spent based on location data emitted from a mobile phone.[133] Prior to this, Kai Biermann noted how our own phones betray us, [134] giving the example of Malte Spitz of the German Green party who published the data that was retained under Germany's data retention laws. Zeit Online created an interactive map which detailed Spitz's movements,[135] based on nearly 36000 data points. [136] Biermann continued that this data revealed:

> [W]hen Spitz walked down the street, when he took a train, when he was in an airplane. It shows where he was in the cities he visited. It shows when he worked and when he slept, when he could be reached by phone and when was unavailable. It shows when he preferred to talk on his phone and when he preferred to send a text message. It shows which beer gardens he liked to visit in his free time. *All in all, it reveals an entire life* (author's emphasis).[137]

In 2011, Mark Gasson *et al* conducted a study[138] of tracking four individuals from three EU Member states via their GPS enabled mobile phones. Their location data were stored in a central database for automated and manual processing (akin to data retention) in order to form profiles. Gasson *et al* noted that based on location data, a job profile could likely be drawn for certain participants.[139] Gasson *et al* were also able to infer the relationship (a business) between two of the participants based on travel patterns.[140] Gasson *et al* were also able to infer that one participant was in some way involved with children, based on trips to the park and kindergarten.[141] Based on routine, Gasson *et al* were also able to infer shopping habits based trips to petrol stations.[142] On the issue of sensitive personal data, Gasson *et al* noted that although determining a participant's religion was inconclusive it may be possible to classify a person's specific religion with some degree of certainty, due to the fact that most mainstream religions have a defined routine, held in identifiable locations.[143] A point that Gasson *et al* note

---

[132] *S and Marper v UK* App nos. 30562/04 and 30566/04 (ECHR, 4 December 2008), [76].
[133] Abdulaziz Almehmadi, (n16), 30-31.
[134] Kai Biermann, 'Betrayed by our own data' (10 March 2011) <http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz> accessed 13 April 2017.
[135] Zeit Online, 'Tell-all telephone' <http://www.zeit.de/datenschutz/malte-spitz-data-retention> accessed 13 April 2017.
[136] Crassh, 'National Mass Communications Data Surveillance and the Law' (9 August 2016) <http://www.crassh.cam.ac.uk/blog/post/national-mass-communications-data-surveillance-and-the-law> accessed 27 November 2017.
[137] Kai Biermann, (n134).
[138] Mark N. Gasson, Eleni Kosta, Denis Royer, Martin Meints, and Kevin Warwick, 'Normality Mining: Privacy Implications of Behavioral Profiles Drawn from GPS Enabled Mobile Phones' (2011) IEEE Transactions on Systems, Man and Cybernetics 41:2 251, 252.
[139] ibid, 255.
[140] ibid, 257.
[141] ibid.
[142] ibid, 258.
[143] ibid.

is that based on just the data examined there was 'real potential for incorrect conclusions being reached based on the data.'[144] This could have significant impact on individuals.[145]

In 2006, using raw GPS data, Lin Liao *et al*[146] were able to make inferences about daily activities and movements and even when routine was broken. Gerald Friedland and Robin Sommer were able to find private addresses of celebrities as well as the origins of otherwise anonymized Craigslist posting from geo-location data.[147] A website called 'I know where your cat lives'[148] uses location data from EXIF images[149] which is uploaded on social media to broadcast where cats live, therefore revealing addresses. Dr Alex Pentland, director of MIT's Human Dynamics Laboratory noted that '[j]ust by watching where you spend time, I can say a lot about the music you like, the car you drive, your financial risk, your risk for diabetes.'[150]

The WP29 highlighted that behavioural patterns 'may also include data derived from the movement patterns of friends, based on the so-called social graph.'[151] van der Hilst noted that there 'is a possibility that the use of location tracking devices causes effects that are so harmful to an individual or to society at large.'[152] In doing nothing, we may 'end up being a society that distrusts, that we break down the social fabric that we call networked groups and allow ourselves to be taken control over by the techno-political elite.'[153] The societal value of privacy is highlighted and the potential for its devaluation to change society forever. This is all the more serious as location data is difficult to anonymise.[154]

(d) Third Party Data

During written evidence to the Joint Committee on the draft Investigatory Powers Bill (JCDIPB) the Home Office noted that there were no proposals being brought forward for the retention of third party data.[155] This section will prove that although there may have been no proposals (when in fact there were),[156] third party data retention is still possible. Third party data is described as 'information that's collected by an entity that doesn't have a direct relationship with consumers'[157] or anyone.[158] Or more specifically, where 'one

---

[144] ibid, 260.
[145] ibid.
[146] Lin Liao, Donald J. Patterson, Dieter Fox and Henry Kautz, 'Building Personal Maps from GPS Data' (2006) Ann. New York Acad. Sci 1093:1 249.
[147] Gerald Friedland and Robin Sommer, 'Cybercasing the Joint: On the Privacy Implications of Geo-Tagging' (2010) <https://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf> accessed 14 April 2017.
[148] <http://www.iknowwhereyourcatlives.com/> accessed 14 April 2017.
[149] Exchangeable image file format for digital still cameras: Exif Version 2.31, (2016) <http://www.cipa.jp/std/documents/e/DC-008-Translation-2016-E.pdf> accessed 14 April 2017.
[150] Robert Lee Hotz, 'The Really Smart Phone' *Wall Street Journal* (New York City, 23 April 2011) <https://www.wsj.com/articles/SB10001424052748704547604576263261679848814> accessed 14 April 2017.
[151] ARTICLE 29 Data Protection Working Party, (n123). 'The 'social graph' is a term indicating the visibility of friends in social networking sites and the capacity to deduce behavioural traits from data about these friends.'
[152] Rozemarijn van der Hilst, (n128), 35.
[153] Katina Michael & M.G. Michael. 'The social and behavioural implications of location-based services' (2011) Journal of Location Based Services 5:3-4 121, 132.
[154] Open Rights Group, 'Cashing in on your mobile? How phone companies are exploiting their customers' data' (4 March 2016) <https://regmedia.co.uk/2016/04/04/cashinginonyourmobile.pdf> accessed 17 April 2017.
[155] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n59), Home Office, para 2, p491.
[156] Written evidence submitted by GreenNet (IPB0063), para 7.
[157] Jack Marshall, 'WTF is third-party data?' (5 February 2014) <https://digiday.com/media/what-is-third-party-data/> accessed 8 April 2017.
[158] J.F. Houpert, 'What You Need To Know About 1st, 2nd and 3rd Party Data' (20 June 2017) <https://www.datacratic.com/blog/first-second-third-party-data> accessed 10 October 2017.

telecommunications operator is able to see the communications data in relation to applications or services running over their network, but where they do not use or retain that data for any purpose.'[159] As noted above, s.87(4)(d) of the IPA 2016 allows third party data to be retained if it is used or retained for a lawful purpose. BT in their written submissions highlight that to obtain third party data from Facebook, it would have to 'examine all the data, including the content.'[160] In order to do this, BT would have to conduct Deep Packet Inspection (DPI) which enables the ISP to access information addressed to the recipient of the communication only.[161] This, as the European Data Protection Supervisor (EDPS) maintains, requires the *interception* of the metadata and *content* (author's emphasis).[162] Therefore, s.87(4)(d) allows data that has been intercepted to be retained and in doing so stretches beyond what is argued to be communications data as DPI can allow the original content of the communication to be reconstructed in full and analysed.[163] There is no indication in the IPA 2016 that such data would be treated as content.

Moreover, this can be imposed on telecommunications operators via s.87(9)(b)(i) by requiring them to process data for the purposes of retention. iiNet (in an Australian context) argued that data retention would force commercial businesses to become agents of the state in storing and safeguarding large databases they have no business need to do so.[164] This is certainly true for UK businesses when one considers that data generated can be obliged.

The WP29 also opined that requirements for operators to retain traffic data which they do not need for their own purposes would constitute a derogation without precedent to the finality/purpose principle.[165]

Steven Dalby noted that it is 'seriously overstated' that service providers engage in data retention for their own purposes to track URLs, source and destination IP addresses, e-mail headers and the like.'[166] However, BT's own Broadband privacy policy indicates that they keep information about how their Broadband *is used*, to manage traffic flows (traffic management), improve services and for marketing purposes (author's emphasis). BT notes that this includes (and therefore is not limited to) IP addresses and other traffic data including websites individuals have visited.[167] They also state that the law requires them to keep certain (not

[159] Explanatory notes to IPA 2016, (n24), para 262.
[160] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n59), BT, para 10, p209.
[161] Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012XX0208(01)> accessed 17 April 2017, para 32.
[162] ibid.
[163] ibid.
[164] iiNet, 'Limited Submission to the Committee' <http://www.aph.gov.au/DocumentStore.ashx?id=cd64d063-5791-4336-8606-0ee36926b8f9&subId=206461> accessed 17 April 2017.
[165] Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)], <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp99_en.pdf> accessed 17 April 2017. See also Article 6 of the Data Protection Directive/Article 5(b) of the GDPR.
[166] Richard Chirgwin,'Telcos renew calls to limit metadata retention' *The Register* (London, 29 July 2014), <http://www.theregister.co.uk/2014/07/29/telcos_renew_calls_to_limit_metadata_retention/> accessed 17 April 2017.
[167] BT Broadband Privacy Policy <https://www.productsandservices.bt.com/products/static/privacy-policy/?page=Broadband> accessed 17 April 2017.

defined) information about service use for 12 months for law enforcement and national security purposes.

There are issues to be taken with the position adopted by BT. Firstly, Sophie Stalla-Bourdillon noted that website names are application-level metadata, and would require DPI to obtain this information,[168] and therefore BT would be conducting interception. Secondly, traffic management is possible without the use of DPI, thus enhancing both privacy and security.[169] Thirdly, BT does not define what it considers traffic data, so it is impossible to deduce just how intrusive the policy is, but there is some indication based on keeping information on 'how' their services are used i.e. as noted, what websites are visited. Fourthly, the EDPS has maintained that traffic management policies other than for maintaining delivery and security of service (including limiting congestion) should require consent.[170] Fifthly, BT have misstated the law, the law does not require them to retain data for 12 months, the law permits the Secretary of State and Judicial Commissioner to oblige them to retain data for 12 months, and more importantly, this fact should not be made public according to s.95(2) of the IPA 2016 unless the Secretary of State has approved (s.95(4) of the IPA 2016). If retaining data for 12 months without a notice served, this would run contrary to data protection and human rights standards. Sixthly, the information BT stores may be used for purposes beyond law enforcement and national security whether the obligation came from s.1 of DRIPA 2014 or s.61(7) of the IPA 2016. Seventhly, and possibly the most worrying is that s.46 of the IPA 2016 could allow this interception in any event. Section 46(2) allows any business (s.46(4)(a)) to conduct interception if it constitutes a legitimate practice reasonably required for the purpose, in connection with the carrying on of any relevant activities for the purpose of record keeping. Subsection 2(b) indicates that this includes communications relating to business activities. Due to being vaguely defined, this essentially allows interception for 'business purposes.' This would fit with the Home Office's narrative in 2009 where they noted that 'DPI is a term used to describe the technical *process whereby many communications service providers currently identify and obtain communications data from their networks for their business purposes* (author's emphasis).'[171] Given the definitions of communication and data noted in s.261(2) and s.263(1) what is to stop for example, another Phorm scandal?[172] This involved BT, TalkTalk and Virgin Media making a deal with Phorm to covertly intercept traffic of their customers. If Regulations are made for business purpose interception, s.87(4)(d) would not apply because this would constitute a lawful purpose for retention. Therefore, this could allow interception of data and its retention[173] unsuspectedly, therefore again, highlighting the severity of interference and that third-party data actually can be retained.

---

[168] Sophie Stalla-Bourdillon, 'What the hell are these metadata? ….Are communications data, traffic data and metadata all the same thing?' (30 October 2014) <https://peepbeep.wordpress.com/2014/10/30/what-the-hell-are-these-metadata-are-communications-data-traffic-data-and-metadata-all-the-same-thing/> accessed 17 April 2017; Sophie Stalla-Bourdillon, Evangelia Papadaki and Tim Chown, (n4), 441.

[169] Mirja Kühlewind, Dirk Kutscher and Brian Trammell, 'Enabling Traffic Management without DPI' (2015) <https://www.iab.org/wp-content/IAB-uploads/2015/08/MaRNEW_1_paper_18.pdf> accessed 17 April 2017.

[170] Opinion of the European Data Protection Supervisor, (n161), para 80.

[171] Home Office, 'Protecting the Public in a Changing Communications Environment, Summary of Responses to the 2009 Consultation Paper'<http://webarchive.nationalarchives.gov.uk/+/http:/www.homeoffice.gov.uk/documents/cons-2009-communication-data/cons-2009-comms-data-responses2835.pdf?view=Binary> accessed 12 October 2017, p15.

[172] Christopher Williams, 'BT and Phorm: how an online privacy scandal unfolded' *The Telegraph* (London, 8 April 2011) <http://www.telegraph.co.uk/technology/news/8438461/BT-and-Phorm-how-an-online-privacy-scandal-unfolded.html> accessed 17 April 2017.

[173] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n59), Open Rights Group, para 125, p1104.

(e) Internet Connection Records

Internet Connection Records are defined in s.62(7) of the IPA 2016 as communications data which may be used to identify or assist in identifying a telecommunications service when a communication occurs and the data that is generated or processed by the telecommunications operator when supplying said service to the sender of the communication. It is essentially a list of our online activity.[174]

Section 62(7) itself does little to highlight this, nor is it further clarified in the explanatory notes, nor does the technical standards of the Internet define them.[175] ICRs do not 'naturally exist within the technical infrastructure of a telecommunications operator' and so would have to make infrastructural changes in order *generate* and retain ICRs (author's emphasis).[176] The Government did indicate that ICRs are 'records of the internet services that have been accessed by a device' for example 'a record of the fact that a smartphone had accessed a particular social media website at a particular time.'[177] The Government further maintained that ICRs do not provide a full browsing history, nor does it reveal every webpage that a person visited or any action carried out on that webpage.[178]

Claiming that ICR does not reveal every webpage visited (which Graham Smith and Open Rights Group think otherwise)[179] does not detract from the fact that they are a truncated form of everyone's[180] web browsing history[181] which can be very revealing.[182] Many have noted that retaining ICR will reveal sensitive personal information, such as political and religious views, sexual orientation, health conditions and spending habits.[183] Liberty and others[184] also noted that equating phone bills with ICRs is a false comparison as they would provide (or at least that is the intention)[185] a detailed record of a 12 month log of websites visited, communications software used, system updates downloaded, desktop widgets used (e.g. calendars, notes), every mobile app used (e.g. Whatsapp, Signal, Google Maps), and logs of any other device

---

[174] Big Brother Watch, 'Internet Connection Records' (March 2016) <https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Internet-Connection-Records.pdf> accessed 10 October 2017; Privacy International, 'The database of you: Internet Connection Records will allow the UK Government to document everything we do online' <https://www.privacyinternational.org/node/1011> accessed 10 October 2017; Liberty, 'Liberty's briefing on 'Internet Connection Records' in the Investigatory Powers Bill for Report Stage in the House of Lords' (October 2016) <https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%20briefing%20on%20ICRs%20for%20Report%20Stage%20in%20the%20House%20of%20Lords.pdf> accessed 10 October 2017.

[175] Written evidence submitted by Gareth Llewellyn on behalf of Brass Horn Communications (IPB0019).

[176] Liberty, (n174), 8; Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n60), BT, p214.

[177] Investigatory Powers Bill, Internet Connection Records, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473745/Factsheet-Internet_Connection_Records.pdf> accessed 17 April 2017.

[178] ibid.

[179] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n59), Graham Smith, para 104, p1230; Open Rights Group, para 67, p1095.

[180] Paul Bernal, (n60).

[181] Paul Bernal, (n69), 249.

[182] Written evidence submitted by The Institute for Human Rights and Business (IHRB) (IPB0035), para 5.3.

[183] ibid; Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n59), Andrews & Arnold Ltd, p58-59, IT-Political Association of Denmark, para 21, p704; Written evidence submitted by Big Brother Watch (IPB0048); Written evidence submitted by Andrews & Arnold Ltd (IPB0011); Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n59), Open Rights Group, para 67, p1095.

[184] Gareth Llewellyn, (n175).

[185] Written evidence submitted by BT (IPB0061).

connecting to the internet, such as games consoles, baby monitors, digital cameras and e-book readers.[186] Due to the absence of definition of an 'internet communications services' noted in s.62(4)(b)(i) and (5)(c)(i) of the IPA 2016,[187] it is likely that a natural meaning would be used and thus potentially very expansive. Acquiring what is considered ICR would also require some form of DPI to intercept all packets to determine what is and what is not communications data.[188] Moreover, this would capture third party data,[189] which again disproves the position of the Home Office regarding not wanting third party data retention.[190] Given that it has been noted that ICRs would require generation for retention, it is important to consider data generation for the purposes of retention.

(f) Generated Communications Data

As noted above, ICR would need to be generated in order to be retained, this however, does not limit the possibilities for other data to be retained. As techUK noted, a CSP may be required to generate data about the location of its users and then store that data purely for the purposes of law enforcement.'[191] Moreover, s.87(9)(b) can place requirements for *obtaining* (including by generation) data for the purpose of retention. Smith asked the question as whether this could mean that a telecommunications operator could obligate a customer or third party to generate data so it could be obtained and retained,[192] such as Sonos (wireless sound system) compelling its customers to accept their new privacy policy (which collects more data e.g. email addresses and location data) or risk their sound system ceasing to function.[193] Telecommunications operators could be obligated to conduct traffic and social network analysis and data mining[194] either to be obtained or generated for retention purposes, increasing the severity of interference.[195] Furthermore, s.87(9)(b) can also impose requirements for the processing of data for retention. This point is highlighted due to the fact that for example, Microsoft's Windows 10[196] raised significant concerns with the WP29. Their concerns were based on some of the personal data collected and further processed within Windows 10, and specifically the default settings or apparent lack of control for a user to prevent collection or further processing of such data.[197] Despite changes proposed to Windows 10, the WP29 were still concerned about

[186] Liberty, (n174), p 7.
[187] Written evidence submitted by Graham Smith (IPB0025), para 19-25.
[188] Written evidence submitted by Exa Networks Limited (IPB0026), para 23-25; Written evidence submitted by IT-Political Association of Denmark (IPB0051), para 21; GreenNet, (n156), para 11; Written evidence submitted by Open Rights Group (IPB0034), para 6.2.3.
[189] Written evidence submitted by IT-Political Association of Denmark, (n188), para 20.
[190] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n59), Home Office, para 2, p491.
[191] ibid, techUK, para 25, p1268.
[192] Written evidence submitted by Graham Smith, (n186), para 28; Graham Smith, 'Illuminating the Investigatory Powers Act' (22 February 2018) <https://www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html> accessed 3 June 2018.
[193] Thomas Claburn, 'Rejecting Sonos' private data slurp basically bricks bloke's boombox' *The Register* (London, 11 October 2017) <https://www.theregister.co.uk/2017/10/11/sonos_privacy_speakers/> accessed 16 January 2018.
[194] Lukas Feiler, 'The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection' (2010) 1(3) EJLT <http://ejlt.org/article/view/29/75> accessed 25 October 2017.
[195] ibid.
[196] Natasha Lomas, 'Windows 10 privacy settings still worrying European watchdogs' *TechCrunch* (Bay Area, 21 February 2017) <https://techcrunch.com/2017/02/21/windows-10-privacy-settings-still-worrying-european-watchdogs/> accessed 24 April 2017.
[197] Article 29 Working Party's letter to Microsoft (12 January 2016) <http://ec.europa.eu/newsroom/document.cfm?doc_id=42572> accessed 24 April 2017.

the level of protection of users' personal data,[198] in which the Dutch Data Protection Authority found a breach of data protection laws in October 2017.[199]

The title for Part 4, which contains the retention powers, refers not to the retention of relevant communications data, but to *certain data*. This implies that retention is not limited to relevant communications data. Given that s.87(9)(b) does not refer to relevant communications data but just 'data,' it may be possible that telecommunications operators could be obliged to obtain/generate and retain data as defined in s.263(1) which includes (and therefore not limited to) data which is not electronic data and any information (whether or not electronic). Therein lies the danger, because data is so broadly defined, it makes the possibilities as to what can be retained, endless, such as speech data allegedly being hoovered up by Instagram.[200] The only example given is that of ICRs, but it is clear that s.87(9)(b) would not be limited to them. For example, it could force zero-logging[201] Virtual Private Networks[202] (VPNs) to now log data by way of generation for the purposes of retention. This would effectively defeat the purpose of their existence (to prevent web histories from being stored and masking locations). This means that data can still be more intrusive than what is considered 'content.' This concern might not be as far away as some might think, Facebook has announced that it seeks to develop technology that would be able to read a person's mind in order to communicate.[203] The risks of using brainwaves to eavesdrop and gain passwords[204] is already here, which is matched by calls for human rights to protect mental privacy, cognitive liberty, mental integrity and psychological continuity.[205] This is an early signpost of how Article 8 and Article 9 (freedom of religion/thought/conscious) interrelate as discussed in Chapter 4 in light of who can be obligated to retain (Chapter 6). Retention of thought data would truly encompass what Caspar

---

[198] Article 29 Working Party's letter to Microsoft (15 February 2017) <http://ec.europa.eu/newsroom/document.cfm?doc_id=42947> accessed 24 April 2017.

[199] Dutch Data Protection Authority, 'Microsoft Windows 10 Home and Pro investigation' (October 2017) https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/public_version_dutch_dpa_informal_translation_summary_of_investigation_report.pdf> accessed 13 October 2017.

[200] Damián Le Nouaille, 'Instagram is listening to you' *The Medium* (25 August 2017) <https://medium.com/@damln/instagram-is-listening-to-you-97e8f2c53023> accessed 1 November 2017.

[201] No web information collected to provide to law enforcement.

[202] Cryptmode, 'Best No Logs VPN' (25 March 2017) <https://cryptmode.com/best-no-logs-vpn/> accessed 25 April 2017.

[203] Olivia Solon, 'Facebook has 60 people working on how to read your mind' *The Guardian* (London, 19 April 2017) <https://www.theguardian.com/technology/2017/apr/19/facebook-mind-reading-technology-f8> accessed 24 April 2017.

[204] Ajaya Neupane, Lutfor Rahman and Nitesh Saxena, 'PEEP: Passively Eavesdropping Private Input via Brainwave Signals' (2017) <https://info.cs.uab.edu/saxena/docs/nrs-fc17.pdf> accessed 5 September 2017; Charlie Osborne, 'How hackers can hijack brainwaves to capture your passwords' *ZDNet* (8 May 2017) <http://www.zdnet.com/google-amp/article/how-hackers-use-brainwaves-to-capture-your-passwords/?utm_content=buffer5b8d1&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer> accessed 5 September 2017; Tom Simonite, 'Using Brainwaves to Guess Passwords' *MIT Technology Review* (Cambridge, Massachusetts, 5 May 2017) <https://www.technologyreview.com/s/604293/using-brainwaves-to-guess-passwords/?set=604330> accessed 5 September 2017.

[205] Marcello Ienca and Roberto Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology' (2017) Life Sciences, Society and Policy 13:5 1; Marcello Ienca, 'Do We Have a Right to Mental Privacy and Cognitive Liberty?' (3 May 2017) <https://blogs.scientificamerican.com/observations/do-we-have-a-right-to-mental-privacy-and-cognitive-liberty/> accessed 11 October 2017; Sarah Richmond, Geraint Rees and Sarah J. L. Edwards, *I Know What You're Thinking: Brain imaging and mental privacy* (Oxford University Press 2012); Jesper Ryberg, 'Neuroscience, Mind Reading and Mental Privacy' (2017) Res Publica 23:2 197; Francis X. Shen, 'Neuroscience, Mental Privacy, and the Law' (2013) Harvard Journal of Law & Public Policy 36:2 653; Woodrow Barfield and Alexander Williams, 'Law, Cyborgs, and Technologically Enhanced Brains' (2017) Philosophies 2:6.

Bowden highlighted when he coined the term 'CCTV for inside your head'[206] with respect to data retention.

(g) The Big Data Elephant in the Room

Ashlin Lee has argued that communications data retention is only the 'tip of the data iceberg' as it is but one example 'of the emerging ecosystem of digital traces, fragments and identifiers that are created as a part of digitally-mediated social interactions.'[207] Lee refers to Big Data (which communications data is crucial for),[208] which the Oxford English Dictionary defines as:

> Extremely large data sets that may be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions.[209]

Though Shoshana Zuboff argues Big Data as of yet has no reasonable definition.[210] Lee continues that it is tempting to focus solely on communications data retention, but to do so would ignore the vast amounts of data being collected and used today and the *social* questions they raise[211] because Big Data systems seem to be connected to the *interests of society as a whole* (author's emphasis).[212]

As Manon Oostveen notes, on a basic level, Big Data clashes with privacy and the protection of personal data because the collection of data in the acquisition phase can reveal intimate details about a person's life.[213] Big Data casts doubt on the distinction between personal and non-personal data, clashes with data minimisation, undermines informed choice,[214] and

---

[206] Caspar Bowden, 'CCTV for inside your head Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation' (2001) <http://europe.rights.apc.org/eu/cctv_for_the_head.html> accessed 24 April 2017.

[207] Ashlin Lee, 'Beyond metadata: the brave new world of big data retention' *The Conversation* (Melbourne, 31 March 2015) <https://theconversation.com/beyond-metadata-the-brave-new-world-of-big-data-retention-38720> accessed 13 October 2017.

[208] David Lyon, 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique' (2014) Big Data & Society 1:2 1, 10; Andrew Clement, Jillian Harkness and George Raine, 'Metadata – both shallow and deep: the fraught key to big data mass state surveillance' (11 May 2016) <http://www.sscqueens.org/sites/default/files/8_clement_harkness_raine-metadata_-shallow_and_deep_-_bds_workshop_report_2016_may_11.pdf> accessed 13 October 2017; Shoshana Zuboff, 'Big Other: Surveillance capitalism and the prospects of an information civilization' (2015) Journal of Information Technology 30:1 75, 79.

[209] Oxford English Dictionary, 'big data' <https://en.oxforddictionaries.com/definition/big_data> accessed 3 June 2018; see also Bart van der Sloot, 'Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?' (2014) JIPITEC 230 '[G]athering massive amounts of data without a pre-established goal or purpose, about an undefined number of people, which are processed on a group or aggregated level through the use of statistical correlations.'

[210] Shoshana Zuboff, (n208), 75.

[211] Ashlin Lee, (n207).

[212] Bart van der Sloot, 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) International Data Privacy Law 4:4 307, 232; Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) Northwestern Journal of Technology and Intellectual Property 11:5 239, 262.

[213] Manon Oostveen, 'Identifiability and the applicability of data protection to big data' (2016) International Data Privacy Law 0:0 1, 4.

[214] Ira S. Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) International Data Privacy Law 3:2 74.

presents a challenge to purpose limitation.[215] Its accuracy has been described as 'contentious.'[216] It has also been argued that European data protection laws are insufficient to deal with Big Data due its dependency on identifiability of an individual and its focus on the individual (which Big Data does not concern itself with).[217]Big Data is likely to only benefit key commercial entities such as Google, Facebook or Amazon, and not society at large,[218] in which divisions in society could intensify,[219] increasing inequality[220] and even threatening democracy,[221] especially with fake news.[222] It is also the foundation of surveillance capitalism (see Chapter 5).[223] Despite this, it has been argued that the ECtHR's approach to Article 8 'could prove indispensable in the age of Big Data'[224] and may 'lay down stricter and more far-reaching rules and obligations than those following from the GDPR.'[225]

For the purposes of the IPA 2016, Big Data would fall under the umbrella term of communications data, which could be retained in three ways. The first is to be found in s.87(b) of the IPA 2016 where retention notices can oblige telecommunications operators to retain *all or any description* of data (therefore, not even limited to Big Data). Thus, for example, Splunk, which uses Big Data[226] to profile individuals to make them uniquely identifiable[227] could be served with a retention notice to retain this data. It also highlights why the definition of 'data'

[215] Waltraut Kotschy, 'The proposal for a new General Data Protection Regulation—problems solved?' (2014) International Data Privacy Law 4:2 274, 280-281.
[216] Manon Oostveen, (n213), 5.
[217] ibid; Bart van der Sloot, (n212), 232.
[218] Manon Oostveen, (n213), 5; danah boyd and Kate Crawford, 'Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon' (2012) Information, Communication & Society 15 665, 673-675; Mark Andrejevic, 'The Big Data Divide' (2014) IJoC 8 1673.
[219] Manon Oostveen, (n213), 5; Eli Pariser, *The Filter Bubble* (Penguin Books 2012); Lee Rainie and Janna Anderson, 'Code-Dependent: Pros and Cons of the Algorithm Age' (8 February 2017) <http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/02/08181534/PI_2017.02.08_Algorithms_FINAL.pdf> accessed 19 October 2017, p63-70.
[220] Mark Andrejevic, (n218); Sarah Brayne, 'Big Data Surveillance: The Case of Policing' (2017) American Sociology Review 82:5 977; Solon Barocas and Andrew D. Selbst, 'Big Data's Disparate Impact' (2016) California Law Review 104 671; Stephen Graham, 'Bridging Urban Digital Divides? Urban Polarisation and Information and Communications Technologies (ICTs)' (2002) Urban Studies 39:1 33; Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For' (2017) Duke Law & Technology Review 16:1 18; Lee Rainie and Janna Anderson, (n219); Kate Crawford and Ryan Calo, 'There is a Blind Spot in AI Research' (2016) Nature 538 311.
[221] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Penguin Books 2017).
[222] Timothy Summers, 'Facebook is killing democracy with its personality profiling data' *The Conversation* (Melbourne, 21 March 2018) <https://theconversation.com/facebook-is-killing-democracy-with-its-personality-profiling-data-93611> accessed 3 June 2018.
[223] Shoshana Zuboff, (n208), 76.
[224] Bart van der Sloot, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"' (2015) Utrecht Journal of International and European Law 31:80 25, 47.
[225] Bart van der Sloot, 'Decisional privacy 2.0: the procedural requirements implicit in Article 8 ECHR and its potential impact on profiling' (2017) International Data Privacy Law 0:0 1, 12.
[226] Splunk, 'Make Machine Data Accessible, Usable and Valuable to Everyone' <https://www.splunk.com/pdfs/company-overview.pdf> accessed 11 October 2017.
[227] Gleb Esman, 'Splunk and Tensorflow for Security: Catching the Fraudster with Behavior Biometrics' (18 April 2017) <https://www.splunk.com/content/splunk-blogs/en/2017/04/18/deep-learning-with-splunk-and-tensorflow-for-security-catching-the-fraudster-in-neural-networks-with-behavioral-biometrics.html> accessed 24 April 2017.

in s.263(1) of the IPA 2016 becomes important, because of the nigh unlimited[228] possibilities of what could be retained.

The second way is via data generation in which s.87(9)(b) could compel a telecommunications operator to *generate* Big Data for the purposes of retention. Big Data generation for policing purposes could be imposed on telecommunication operators because they are often 'overwhelmed by the sheer volume of data collected through digital surveillance methods, and lack the technological capabilities to use it for operational purposes.'[229] This runs the risk of retaining data that produces biased[230] results based on race,[231] (as the ECtHR has previously acknowledged)[232] gender and socio-economic background.[233] Due to the vagueness of s.87(9)(b), there is no detail on how this (or what) is to be achieved, and thus the secretive[234] algorithms used,[235] which can be artificially intelligent.[236]

The third, is under what constitutes entity data. The JCDIPB referred to LINX's submission on entity data being exceptionally broad as it could include anyone interacting over a telecommunications operator's network. [237] This would be wider still because of the definition of telecommunications operator (see Chapter 6) would encompass companies such as Apple, Facebook, Google, Microsoft, Yahoo! and others and everything they knew about everyone.[238] The JCDIPB acknowledged that given the sophisticated automated profiling of users undertaken by such companies, it would not be difficult to see how entity data would be considerably *more detailed and intrusive* than subscriber data as envisaged in RIPA 2000 (author's emphasis).[239] The potential detail of entity data based upon the detailed automated profiles created was of great concern to the JCDIPB.[240]

Continuing with entity data, David Lyon highlights social media sucks up data of ordinary users' social activities to be quantified and classified, *Big Data goes beyond this* (author's

---

[228] The only limitation would seem to be what is technically possible.
[229] Alexander Babuta, 'Big Data and Policing An Assessment of Law Enforcement Requirements, Expectations and Priorities' (September 2017) <https://rusi.org/sites/default/files/201709_rusi_big_data_and_policing_babuta_web.pdf> accessed 19 October 2017, p26.
[230] Cathy O'Neil, 'The era of blind faith in big data must end' (April 2017) <https://www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end#t-786714> accessed 17 October 2017.
[231] Kate Crawford and Ryan Calo, (n220), 312; Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, 'Machine Bias' *ProPublica* (Ney Work City, 23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 19 October 2017.
[232] *Gillan and Quinton v UK* App no. 4158/05 (ECHR, 12 January 2010), [85].
[233] Solon Barocas and Andrew D. Selbst, (n220).
[234] Lilian Edwards and Michael Veale, (n220); Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press, Cambridge, MA, 2015); Danielle Keats Citron and Frank A. Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) Washington Law Review 89:1 1.
[235] Salvador García and Julián Luengo, 'Tutorial on practical tips of the most influential data preprocessing algorithms in data mining' (2016) Knowledge-Based-Systems 98 1.
[236] Wolfie Christl, 'How Companies Use Personal Data Against People' (October 2017) <http://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf> accessed 17 October 2017, 13. See also Chapter 4.
[237] Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill*, (n61), 70.
[238] ibid; Cathy O'Neil, (n221), 181.
[239] Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill*, (n61), 71.
[240] ibid, 72.

emphasis).[241] Many corporations seek to capitalise on Big Data[242] as it 'draws on data streams from social and online media as well as personal devices designed to share data.'[243] For example, Facebook's social graph, 'a global mapping system of users and how they are related to each other' and the biggest on the planet[244] has been likened to practices of the Stasi.[245] In 2011 it was pointed out that Facebook stores up to *800 pages* of personal data *per* user account which includes *deleted* messages, events *not attended* and *every machine* used to log into Facebook with (author's emphasis).[246] Similarly, Judith Duportail demonstrated that Tinder kept *800* pages of her online dating behaviour (author's emphasis).[247] Google is the largest and most successful Big Data company because it is the most visited website, thus having the largest data exhaust.[248] It also is largely the reason the explosion in attractiveness of Big Data analytics.[249] Big Data analytics is not just conducted by Google and Facebook, but many other large internet-based firms and appears to be the default model for most online startups and applications.[250]

Big Data analytics is also prevalent in marketing, finance, insurance, at work, through devices and platforms, data brokers,[251]government and corporate databases, and private and public surveillance cameras.[252]

Therefore, the main difference between communications data (as discussed before this subsection) and Big Data, is that with the latter, the data is *already* aggregated,[253] the mosaic[254] notion of communications data, and the profiles built from them are *readily available*. Thus, the *sensitive profiles of an individual's actions and intentions* are readily retainable, further increasing the severity of interference. As Fisher et al put it, 'big data analytics is a workflow that distills terabytes of low-value data…down to, in some cases, a single bit of high-value data.'[255] As Feiler points out 'everybody's communicational behaviour would be automatically

---

[241] David Lyon, (n208), 4.
[242] ibid, 5.
[243] Kirstie Ball, 'Consumer Surveillance and Big Data' <http://www.sscqueens.org/sites/default/files/9_consumer_surveillance_and_big_data-kirstie_ball.pdf> accessed 13 October 2017.
[244] David Lyon, (n208), 8.
[245] Owen Mundy, 'Stasi networks and Facebook Social Graph' (28 May 2017) <http://owenmundy.com/blog/2017/05/stasi-facebook-big-data-daad-day-17-stasi-networks-and-facebook-social-graph/> accessed 13 October 2017.
[246] Matthew Humphries, 'Facebook stores up to 800 pages of personal data per user account' (28 September 2011) <https://www.geek.com/geek-pick/facebook-stores-up-to-800-pages-of-personal-data-per-user-account-1424807/> accessed 30 October 2017.
[247] Maryant Fernández Pérez, 'Tinder and me: My life, my business' (4 October 2017) <https://edri.org/tinder-my-life-my-business/> accessed 1 November 2017.
[248] Shoshana Zuboff, (n208), 79.
[249] ibid.
[250] ibid, 77.
[251] Wolfie Christl and Sarah Spiekermann, *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy* (Facultas.Wuv Universitäts 2016), 25-118.
[252] Shoshana Zuboff, (n208), 78-79.
[253] Paul Benral, (n69), 248.
[254] 'Mosaic theory describes the concept that individual actions may not rise to the level of a search in and of itself, but may constitute a search when aggregated' See Bethany. L. Dickman, 'Untying Knotts: The Application of Mosaic Theory to GPS Surveillance in UNITED STATES V. MAYNARD' (2011) American University Law Review 60:3, 731, n15
[255] Danyel Fisher, Rob DeLine, Mary Czerwinski and Steven Drucker, 'Interactions with Big Data Analytics' (2012) Interactions 19:3 50.

analyzed for certain 'suspicious' communication patterns - irrespective of any anterior suspicion.'[256]

The bias in Big Data to be retained could be based on what telecommunications are obligated to generate for law enforcement (due to ethnic profiling,[257] which can intensify ethnic profiling)[258] or inherent within the operations of the telecommunications operators.[259]

(h) Big Data, Group Privacy, the social value of Privacy and Article 8 ECHR

Taylor *et al* noted that in the era of Big Data 'where analytics are being developed to operate at as broad a scale as possible, the individual is often incidental to the analysis' but instead are directed at the 'group level.'[260] As van der Sloot notes, Article 34 ECHR allows *groups* to make applications to the ECtHR.[261] van der Sloot continues that 'large groups are or *society as a whole* is affected and that group or societal interests are undermined' by Big Data processes (author's emphasis).[262]This reference to society allows for an important discussion on the social value of privacy and Article 8. Solove notes that privacy is a recognition that in certain circumstances it is in society's best interests to curtail the power of its norms, in protecting the individual for the good of society.[263] It has been argued that 'that a sociological analysis is useful in illuminating aspects of human rights law in ways that remain largely absent in legal scholarship.'[264]Regan regarded privacy a common value because we all recognise its importance in our lives, a public value because it is necessary to the proper functioning of a democratic political system, and a collective value because technology and market forces make it increasingly difficult for any of us to have privacy unless we all have

---

[256] Lukas Feiler, (n194).
[257] *Gillan and Quinton v UK*, (n232); *S and Marper*, (n132), [38-40] and [124]; Bart van der Sloot, Dennis Broeders and Erik Schrijvers, *Exploring the Boundaries of Big Data* (Amsterdam University Press, Amsterdam 2016), 125; Bernard E. Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* (Chicago: University of Chicago Press 2007); Olivier De Schutter and Julie Ringelheim, 'Ethnic Proϕling: A Rising Challenge for European Human Rights Law' (2008) Modern Law Review 71:3 358; Open Society Initiative, 'Equality under Pressure: The Impact of Ethnic Profiling' (2013) <https://www.opensocietyfoundations.org/sites/default/files/equality-under-pressure-the-impact-of-ethnic-profiling-netherlands-20131128_1.pdf> accessed 19 October 2017; Leanne Weber and Ben Bowling, *Stop and Search: Police Power in Global Context* (Routledge 2012); Bart Custers, Tal Zarsky and Bart Schermer, *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases (Studies in Applied Philosophy, Epistemology and Rational Ethics)* (Springer, Heidelberg 2013).
[258] Bart van der Sloot, Dennis Broeders and Erik Schrijvers, (n257), 125; Joanne P. van der Leun and Maartje A.H. van der Woude, 'Ethnic profiling in the Netherlands? A reflection on expanding preventive powers, ethnic profiling and a changing social and political context' (2011) Policing and Society 21:4 444; Open Society Initiative, (n257).
[259] Lee Rainie and Janna Anderson, (n219), p57. Latanya Sweeney, 'Discrimination in Online Ad Delivery' (28 January 2013) <https://arxiv.org/pdf/1301.6822.pdf> accessed 19 October 2017; Paul Bernal, (n69), 257-258; Stephen Buranyi, 'Rise of the racist robots – how AI is learning all our worst impulses' *The Guardian* (London, 8 August 2017) <https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses> accessed 19 October 2017. See also discussion on discrimination in Chapter 4.
[260] Linnet Taylor, Luciano Floridi, and Bart van der Sloot, 'Introduction: A New Perspective on Privacy' in Linnet Taylor, Luciano Floridi, and Bart van der Sloot (eds) *Group Privacy New Challenges of Data Technologies* (Springer Nature 2017), 2.
[261] Bart van der Sloot, '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 Linnet Taylor, Luciano Floridi, and Bart van der Sloot (eds) *Group Privacy New Challenges of Data Technologies* (Springer Nature 2017), 199.
[262] ibid, 217.
[263] Daniel Solove, *Understanding Privacy*, (n47), 94.
[264] Paul Johnson, 'Sociology and the European Court of Human Rights' (2014) Sociological Review 62:3 547, 561.

privacy at a similar level.[265] Hughes builds on the latter two aspects highlighting that privacy is good for democracy and in terms of voter autonomy and its attraction of talented people to public office.[266] Privacy fosters autonomous individuals, providing them with space to develop opinions and ideas (such as this thesis), which in turn improves society as a whole.[267] Privacy is also important for ideas unconnected to democratic functions connected to broader autonomy based activities such as freedom of speech and building different types of social relations.[268] Malloggi argues that if we fail to protect the sphere of social relationships, we may also fail to defend a democratic state,[269] and an attack on privacy is consequently an attack on autonomy.[270] Malloggi argues that post-Snowden 'we know that the privacy of citizens has been disregarded' by the US and EU.[271] For Malloggi, privacy is the substratum of *every* social relationship, and if privacy is defended for a group, it means that we preserve the individual's autonomy because surveillance at group level is dangerous for the maintenance of a democratic society and the freedom of expression which conditions it.[272]van der Sloot adds that although the ECtHR has not recognised group privacy (grouping based upon algorithms etc that salient features of interest, according to some particular purpose)[273] as such, they have accepted that large groups and entire towns can complain under Article 8.[274] Forgetfulness (due to data retentions endurance) is not just an individual good, but a social good.[275] They contend that a world where everything one does is recorded and never forgotten is not a world conductive to the development of democratic citizens.[276]

(i) An Example of the retention of the any or all description of data: Session-Replay Scripts and Password Managers

Section 87(2)(b) of the IPA 2016 can be used to oblige telecommunications operators to retain all or any description of data. For the purposes of this Chapter, Session-Replay Scripts will be used as an example. Session-Replay scripts are third-party website analytic scripts that record keystrokes, mouse movements, scrolling behaviour along with the contents of the page visited.[277] Englehardt *et al* note this could include information regarding medical conditions, credit card details, passwords *without* submission of said information liking it to someone looking over your shoulder (author's emphasis).[278] Englehardt *et al* also demonstrated how third-party scripts could exploit web browser's password managers by extracting usernames

[265] Priscilla M. Regan, *Legislating Privacy, Technology, Social Values and Public Policy* (The University of North Carolina Press 1995).
[266] Kirsty Hughes, 'The social value of privacy, the value of privacy to society and human rights discourse' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy Interdisciplinary Perspectives* (Cambridge University Press 2015), 228-229.
[267] ibid, 229.
[268] ibid.
[269] Francesca Malloggi, 'The Value of Privacy for Social Relationships' (2017) Social Epistemology Review and Reply Collective 6:2 68, 70.
[270] ibid, 72.
[271] ibid.
[272] ibid, 74.
[273] Bart van der Sloot, (n261), 7.
[274] ibid, 215.
[275] Jean-Francois Blanchette and Deborah G. Johnson, 'Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness' (2002) The Information Society 18 33, 34-35.
[276] ibid, 36.
[277] Steven Englehardt, Gunes Acar, and Arvind Narayanan, 'No boundaries: Exfiltration of personal data by session-replay scripts' (15 November 2017) <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/> accessed 15 November 2017.
[278] ibid.

and passwords.[279] Websites using such third-party scripts would fall under retention obligations as they would be considered telecommunications services.[280]This would only serve to highlight another way in retention of communications data at the very least puts it on par with interception of content.

3.5 Interference based upon whom has access

As Roberts noted above, interference posed by data retention cannot solely be based upon the nature of the data but whom has access. The ECtHR has stressed that the risk of abuse is intrinsic to any system of secret surveillance.[281] The CJEU in *Digital Rights Ireland* referred to the ECtHR's jurisprudence on the risk of unlawful access and use of said data[282] and AG Saugmandsgaard Øe highlighted the very real risk of abusive or illegal access to retained data based on the 'extremely high' number of requests by Sweden and the UK.[283] As Bernal notes, once data is gathered, the risks of misuse, misappropriation, hacking, loss, corruption, error and function creep become more apparent.[284] Under the IPA 2016 many public authorities now have access to retained data for which sufficient justification has not been made[285] which is a concern.[286] Moreover, outside of the bodies that have lawful access, the vulnerability to e.g. hacking serves to increase the severity of interference posed.

3.6 Conclusions

This section has considered specific types of communications data, and more general observations to reveal just how intrusive they are. It was highlighted that two types of communications data, username and password, in and of themselves was enough to render communications data more intrusive than content, because obtaining this would completely compromise the individual or user. It also highlighted how intrusive other forms of communications data can be for example, location data which can lead to revealing sensitive personal data. Consideration was also given to the fact the retention of ICRs and third party data would require interception, the very thing that would make available the content of communications. These types of communications data can also reveal sensitive personal data and habits. Finally, as it was noted that for ICRs to exist, they would have to be generated, but it was highlighted that ICRs are not the only type of data that could be generated as Part 4 leaves the possibility for other unknown types of data (such as mind data) which are not limited to relevant communications data to be retained. Communications data such as ICRs,[287] entity data,[288] and all and any description of data extend well beyond the data types to be retained at

---

[279] Gunes Acar, Steven Englehardt, and Arvind Narayanan, 'No boundaries for user identities: Web trackers exploit browser login managers' (27 December 2017) <https://freedom-to-tinker.com/2017/12/27/no-boundaries-for-user-identities-web-trackers-exploit-browser-login-managers/> accessed 2 January 2018.
[280] See Chapter 6.
[281] *Uzun*, (n40), [61]; *S and Marper*, (n132), [99].
[282] *Digital Rights Ireland*, (n35), [54-55).
[283] Opinion of Saugmandsgaard Øe, (n64), [260].
[284] Paul Bernal, (n69), 251.
[285] See Chapter 7.
[286] Joseph Cox, 'Even the Food Standards Agency Could Access UK Surveillance Data Under New Bill' *Motherboard* (Montreal, 26 November 2015) <https://motherboard.vice.com/en_us/article/ezpddn/even-the-food-standards-agency-could-access-uk-surveillance-data-under-new-bill> accessed 27 November 2017.
[287] Graham Smith, 'Data retention - the Advocate General opines' (19 July 2016) <http://www.cyberleagle.com/2016/07/data-retention-advocate-general-opines.html> accessed 5 January 2018.
[288] Home Office, 'Investigatory Powers Act 2016 Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data' (November 2017)

an EU level. Said data could and would also be more intrusive than the content of communications.

The Interception of Communications Commissioner (IoCC) in a report detailed:

> **761,702** items of communications data were acquired by public authorities during 2015. An item of data is a request for data on a single identifier or other descriptor, for example, **30 days of incoming and outgoing call data in relation to a mobile telephone would be counted as one item of data**.[289]

Given what could be revealed from telephone data mentioned above[290] it demonstrates how intrusive powers can be masked, when in reality the amount of items of data could be in the hundreds or thousands. Would 12 months of call data also only be classed as one item of data? This one item of data could tell public authorities a great deal about the individual concerned. A long enough history of phone communications data can be used to determine socioeconomic status, and can 'accurately reconstruct the distribution of wealth of an entire nation or to infer the asset distribution of microregions composed of just a few households.'[291] This will only intensify with what is now considered under the umbrella term of communications data. This relates back to the mosaic notion of communications data in which the cumulative total of different types of communications data[292] has to be considered. Such data may be used to predict gender, age group, marital status, job and number of people in the household,[293] it can uncover the hidden patterns of our social lives, travels, risk of disease—even our political views.[294]

The UN Office of the High Commissioner for Human Rights (OHCHR) also felt the distinction between communications data and content were no longer persuasive because it can go *beyond even that conveyed by accessing the content of a private communication* (author's emphasis).[295]

This intrusiveness intensifies further because communications data is already parsed in a computer-readable form that allows it to be combined with billions of other pieces of communications data,[296] particularly in light of Big Data'[297] which provides a 'God's eye view

---

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663668/November_2017_IPA_Consultation_-_consultation_document.pdf> accessed 5 January 2018, 10-11.

[289] Report of the Interception of Communications Commissioner, 'Annual Report for 2015' (8 September 2016) <http://iocco-uk.info/docs/56850%20HC%20255%20ICCO%20Web%20only.pdf> accessed 18 April 2017, para 7.23.

[290] Jonathan Mayera, Patrick Mutchlera, and John C. Mitchella, (n57).

[291] Joshua Blumenstock, Gabriel Cadamuro and Robert On, 'Predicting poverty and wealth from mobile phone metadata' (2015) Science 350:6264 1073.

[292] Matthew White, (n80), 9.

[293] Sanja Brdar, Dubravko Ćulibrk, Vladimir Crnojević, 'Demographic Attributes Prediction on the Real-World Mobile Data' (June 2012) <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.296.1374&rep=rep1&type=pdf> accessed 14 April 2017.

[294] Robert Lee Hotz, (n150).

[295] The right to privacy in the digital age, Report of the Office of the High Commissioner for Human Rights, (2014) <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf accessed 24 April 2017, para 19.

[296] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n59), Jamie Dowling, para 7.1, p342.

[297] Paul Bernal, (n69), 248.

of ourselves.'[298] Big Data analysis is possible through retaining *all or any description* of data, the generation and obtaining of communications data and entity data. This includes traffic, social network analysis, and data mining which together would 'allow for fishing expeditions and a continuous surveillance of the entire population,'[299]a situation Judge Pettiti warned against[300] many years before. One in ten business in the EU (and 15% of UK businesses) analyse Big Data[301] and this is likely to increase.

Also, even if one were to follow this arbitrary distinction in intrusiveness, iiNet has demonstrated that embedded data about communications like Twitter, Facebook, and websites does in fact reveal content of communications (such as tweets), and lots of it.[302] Therefore, even taking into account the CJEU's restrictive approach on the essence of right in comparison to data retention and access to content, making such a distinction becomes more unconvincing.[303] Moreover, in *Digital Rights Ireland* the CJEU did not examine profiling or analytical use of data (which Big Data by itself allows) which *does* touch upon the essence of the right to privacy and others.[304] It was also demonstrated that access to retained data should factor into the severity of interference with the rights in question.

In *R.E v United Kingdom*[305] the ECtHR acknowledged that it generally only applies strict criteria with regards to interception cases, but accepted this would depend on the circumstances of the case at hand and the level of interference with Article 8.[306]The ECtHR continued that it has not excluded the principles developed in interception jurisprudence as the divisive factor would be the level of interference and *not* the technical definition of that interference (author's emphasis).[307] This would be consistent with the ECtHR's 'pragmatic, common-sense approach rather than a formalistic or purely legal one.'[308]

Although this case concerned covert-surveillance, such a position can be applied to communications data which is supported by the ECtHR in *Szabo* where it was maintained that:

> Given 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 protection of private life even more acutely* (author's emphasis).[309]

---

[298] Alex Pentland, 'Society's Nervous System: Building Effective Government, Energy, and Public Health Systems' (2012) Computer 45:1 31, 37.
[299] Lukas Feiler, (n194).
[300] *Kopp v Switzerland* App no. 23224/94 (ECHR, 25 March 1998); Stephen Uglow, 'The Human Rights Act 1998: Part 4: covert surveillance and the European Convention on Human Rights,' [1999] Criminal Law Review 287, 289.
[301] Eurostat, '1 in 10 EU businesses analyses big data' (16 May 2017) <http://ec.europa.eu/eurostat/web/products-eurostat-news/-/EDN-20170516-1?inheritRedirect=true&redirect=%2Feurostat%2F> accessed 27 October 2017.
[302] iiNet, 'Protecting your privacy: Our stand against 'mandatory data retention'' (21 July 2014) <http://blog.iinet.net.au/protecting-your-privacy/> accessed 30 December 2016.
[303] Matthew White, (n80), 25.
[304] Douwe Korff, 'Passenger Name Records, data mining & data protection: the need for strong safeguards' (15 June 2015) <https://rm.coe.int/16806a601b> accessed 6 November 2017, p93-94.
[305] *R.E. v United Kingdom* App no. 62498/11 (ECHR, 27 October 2015).
[306] ibid, [127].
[307] ibid, [130].
[308] *Botta v Italy* App no. 21439/93 (ECHR, 24 February 1998), [27].
[309] *Szabo and Vissy v Hungary* App no. 37138/14 (ECHR, 12 January 2016), [53].

This demonstrates that even if the UK considers communications data as less revealing than content, a human rights approach will consider the impacts of rights, and not constrain itself to technical definitions. This is even more so as the ECHR is regarded as a 'living instrument' in which it must be interpreted in the light of present-day conditions.[310] Lestas notes the 'living instrument' has shifted from 'commonly accepted standards in domestic legislation to signs of evolution of *attitudes* amongst modern societies (author's emphasis).'[311] Given that Chapter 4 will highlight that privacy and data protection are valued by individuals and society, this should also inform the ECtHR's interpretation. Furthermore, the ECHR must not be confined to the intentions of their authors as expressed many decades ago.[312] What is more, the ECtHR noted with regards to its own case law that a failure to maintain a dynamic and evolutive approach would risk rendering it a bar to reform or improvement.[313] Alastair Mowbray welcomes the ECtHR's creativity regarding the interpretation and application of the Convention**.**[314] Such creative interpretation should guide the ECtHR to conclude that communications data is just as if not more intrusive than access to the content. Given that the ECtHR already takes a robust approach to data protection[315] the use of new technologies in surveillance and databases,[316] this evolution would be consistent. This would also fall in line with AG Saugmandsgaard Øe's opinion in *Tele2 and Watson* that in the individual context, a general data retention obligation would facilitate equally serious interferenc*e*s as interception. To add further weight to this point, data retention will involve some form of interception depending on what communications data is sought. The ECtHR applies stricter standards regarding interception,[317] and thus the same standards should apply here. As judge Pettiti in *Malone* articulated that the ECtHR:

> [F]ulfils that function by *investing Article 8…with its full dimension* and by *limiting the margin of appreciation especially* in those areas *where the individual is more and more vulnerable as a result of modern technology* (author's emphasis).[318]

Chapter 5 will detail further why the same strict standards of interception should apply to data retention due to both constituting secret surveillance. This Chapter has also demonstrated ways in which communications data can create a more serious interference. In conclusion, there is at least an arguable[319] case that data retention as envisaged in the IPA 2016 adversely effects the essence of rights that are interfered with has been made. Wisman, in the opinion of the author is correct in concluding that data retention 'is the codification of arbitrariness and *therefore irreconcilable with the essence of the right to private life*.'[320] The CJEU should reconsider their position on this and have the opportunity to do so given the preliminary reference from the IPT.[321] Given the ECtHR's position in *Big Brother Watch*, it should no

[310] *Tryer v United Kingdom* App no. 5856/72 (ECHR, 25 April 1978), [31].
[311] George Lesta, *A Theory of Interpretation of the European Convention on Human Rights* (Oxford University Press, 2007), 77.
[312] *Loizidou v Turkey* App no. 15318/89 (ECHR, 23 March 1995), [71].
[313] *Stafford v United Kingdom* App no. 46295/99 (ECHR, 28 May 2002), [68-69].
[314] Alastair Mowbray, 'Creativity of the European Court of Human Rights' (2005) Human Rights Law Review 5:1 57, 79.
[315] Thérèse Murphy and Gearóid Ó Cuinn, 'Works in Progress: New Technologies and the European Court of Human Rights' (2010) HRLR 10:4 601, 638.
[316] ibid, 636.
[317] *Uzun*, (n40), [66].
[318] *Malone v UK* App no. 8691/79 (ECHR, 2 August 1984), Concurring Opinion of Judge Pettiti.
[319] Crassh, (n136).
[320] Tijmen Wisman, 'Privacy: Alive and Kicking' (2015) European Data Protection Law Review 1:1 80, 84.
[321] *Privacy International v the Secretary of State for Foreign and Commonwealth Affairs and Others* [2017] IPT/15/110/CH, [72].

longer be a question of should the ECtHR apply the standards of interception to data retention, but they *must* as a matter of necessity.

Both the OHCHR and ECtHR spoke of communications data in terms of privacy etc, however, as noted above, in order to retain certain communications data, DPI will have to be used and in this regard Fuchs noted that we do not only need privacy and data protection assessments, but *broader societal impact assessments* (author's emphasis).[322] This reaffirms the notion that privacy has a societal importance, and furthermore, privacy and even data protection, are not the only fundamental rights that need to be considered because 'the *human rights impact* of data retention on the ability to create profiles, or to confirm a future suspicion, has rightly been highlighted as a *human rights* risk (author's emphasis).'[323] The next Chapter discusses the implications of data retention on *other* fundamental rights as well as privacy and data protection. An ECHR perspective becomes all the more important as communications data retained[324] by information society services[325] and entity data[326] falls outside the scope of *Tele2 and Watson*.[327] This would not be the case under the ECHR.

[322] Christian Fuchs, 'Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society' (2012) <http://www.projectpact.eu/privacy-security-research-paper-series/%231_Privacy_and_Security_Research_Paper_Series.pdf> accessed 21 April 2017.
[323] Emily Taylor, 'The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality' (January 2016) <https://www.cigionline.org/sites/default/files/gcig_no24_web_2.pdf> accessed 19 October 2017.
[324] Sophie Stalla-Bourdillon, Evangelia Papadaki and Tim Chown, (n4).
[325] See Chapter 6.
[326] *Liberty*, (n35), [151].
[327] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-970.

Chapter 4: Data Retention, a fundamental rights issue? Article 8 ECHR and Article 7 EU Charter underpinning democracy in the digital age?

4.1 Introduction

It must be noted that from the outset, as the previous Chapter indicated, the types of data that can be retained under Part 4 of the Investigatory Powers Act 2016 (IPA 2016) includes communications data *and* content.

This Chapter seeks to highlight that data retention affects not just privacy or private life, but other fundamental rights such as freedom of expression and religion. This approach will consider rights protected under the European Convention on Human Rights (ECHR) and the European Union's (EU) Charter of Fundamental Rights (CFR). Article 8 ECHR and it's CFR equivalent, Article 7 will be considered given that the latter has the same meaning and scope,[1] thus reference to Article 8 includes Article 7. Establishing that data retention interferes with Article 8 ECHR/7 CFR, leads to arguing further that private life encompasses more than just privacy. An in-depth analysis of private life case law is considered to highlight the multiple ways in which data retention threatens it. This will also be the case for family life and correspondence. 'Home' will be discussed in Chapter 6, whereas the data protection aspect of Article 8 will be discussed here also. This is specifically protected by Article 8 CFR.

Exclusively focussing on Article 8, (which is usually considered as the main human right that bears the brunt of surveillance interferences)[2] would be a disservice to the issues at hand. Surveillance has pervasive effects 'on several other human rights.'[3] Paul Bernal notes that privacy is only one aspect of surveillance because it impacts on *other* fundamental rights. Bernal notes that surveillance impacts upon freedom of expression, association, and religion. He also notes that surveillance can impact upon a fair trial, and can also have discriminatory implications.[4] This necessitates an assessment of the types of data retained and its impact upon Article 9-11, 14 and 6 ECHR. Article 2 Protocol 4 will also be considered given the importance of location data discussed in Chapter 3. In addition to Chapter 3, it demonstrates further just how serious of an interference the types of data retained poses to fundamental rights. Each of these rights are important for a functioning democracy, and Article 8 underpins them all. This also builds on the idea of the social value of privacy and its importance to democracy through legal analysis.

The then United Nations High Commissioner for Human Rights (UNHCHR), Ms. Navi Pillay, commented in an expert seminar that digital communications technologies have become part of the very fabric of our everyday lives.[5] Due to information technology innovations, there has

[1] Article 52(3) of the CFR.
[2] Antonella Galetta, 'The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?' (2013) European Journal of Law and Technology 4:2 <http://ejlt.org/article/view/221/377> accessed 16 May 2017.
[3] ibid.
[4] Paul Bernal, 'Data gathering, surveillance and human rights: recasting the debate' (2016) Journal of Cyber Policy 1:2 243, 252-260.
[5] Opening Remarks by Ms. Navi Pillay United Nations High Commissioner for Human Rights to the Expert Seminar: The right to privacy in the digital age, (24 February 2014), Room XXI, Palais des Nations, Geneva,

been a dramatic improvement in real-time communications and information sharing, which in turn foster democratic participation thereby improving human rights.[6] There was, however, a flip side, in that such new technologies are vulnerable to mass surveillance. There are even new technologies covertly designed (such as the Evident Tool, made by BAE)[7] for the purpose of facilitating said surveillance which in turn threaten individual rights such as privacy, freedom of expression, association and thus inhibits the free functioning of a vibrant civil society.[8] The importance of the UNHCHR's comments highlighted, albeit briefly, that what is at stake is not just the notion of privacy, but other fundamental rights and the functioning of society. Though it has been argued, and will continue to be argued, that privacy is more than just an individual right, it is true that data retention is a threat to the free functioning of a vibrant civil society. This is precisely why the United Nations (UN) and Council of Europe (CoE) have rightly argued 'that the rights held by people offline must also be protected online.'[9]

4.2 Article 8: The right to respect for private and family life, home and correspondence

Article 8 states:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society…

Private and family life and correspondence will be considered in this Chapter. The threshold for interference is not an especially high one,[10] and such justification[11] for interferences does not necessarily have to be factual.[12] Private and family life, and correspondence is interfered with by:

> [T]he mere *existence* of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; *this menace necessarily strikes*

<http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=E> accessed 14 February 2017.

[6] ibid.

[7] Rob Evans, 'BAE 'secretly sold mass surveillance technology to repressive regimes'' *The Guardian* (London, 15 June 2017) <https://www.theguardian.com/business/2017/jun/15/bae-mass-surveillance-technology-repressive-regimes> accessed 5 November 2017.

[8] Ms. Navi Pillay, (n5).

[9] ibid; United Nations General Assembly, 'The promotion, protection and enjoyment of human rights on the Internet' (27 June 2016) <https://www.article19.org/data/files/Internet_Statement_Adopted.pdf> accessed 25 April 2017; Resolution 68/167 adopted by the General Assembly on 18 December 2013, 'The right to privacy in the digital age' (21 January 2014) <http://undocs.org/A/RES/68/167> accessed 25 April 2017; Council of Europe, 'Human Rights for Internet Users' <https://www.coe.int/en/web/internet-users-rights/guide> accessed 28 April 2017.

[10] *AG (Eritrea) v Secretary of State* [2007] EWCA Civ 801, [28].

[11] Douwe Korff, 'The Standard Approach Under Articles 8-11 ECHR and Article 2 ECHR' (2009) <http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf> accessed 5 November 2017.

[12] Ivana Roagna, 'Protecting the right to respect for private and family life under the European Convention on Human Rights' (2012) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806f1554> accessed 6 April 2017, p35.

> *at freedom of communication between users of* the postal and *telecommunication services* (author's emphasis).[13]

This supports van der Schyff's view, who has argued for a wider interpretation of a right's scope because a narrow interpretation would essentially leave the applicant with the difficult task of proving that their right had been interfered with.[14] A wider interpretation would intensify the onus on the Member State to justify why it had interfered with the applicant's right in the first place, placing the State on guard in consciously having to respect people's rights.[15]

In *Colon v Netherlands*[16] the European Court of Human Rights (ECtHR) noted in relation to Article 34[17] where it was noted that in principle, it is not sufficient to claim to be a victim under Article 34 ECHR by the mere existence of legislation but it does entitle:

> [I]ndividuals to contend that legislation violates their rights by itself, in the absence of an individual measure of implementation, if they run the risk of being directly affected by it; that is, if they are required either to modify their conduct or risk being prosecuted, or if they are members of a class of people who risk being directly affected by the legislation.

This raises the interesting question of whether widespread data retention would have the same effect because citizens are left with either abstaining from using the internet or other common electronic communications channels or face the risk of being subject to surveillance.[18] The Romanian Constitutional Court accepted this 'take it or leave it' approach to technology use and data retention.[19]

Ursula Kilkelly notes that Article 8 concepts are dynamic insofar as their meaning is capable of evolving and also, that they have the potential to embrace a wide variety of matters, some of which are connected with one another and some of which overlap.[20] The following subsections will detail why various aspects of Article 8 are interfered with, starting with private life.

(a) Private life

---

[13] *Klass v Germany* App no. 5029/71 (ECHR, 6 September 1978), [41].
[14] Gerhard van der Schyff, 'Interpreting the protection guaranteed by two-stage rights in the European Convention on Human Rights: The case for wide interpretation' in Eva Breams and Janneke Gerards (eds) *Shaping Rights in the ECHR: The Role of the European Court of Human Rights in Determining the Scope of Human Rights* (Cambridge University Press 2013), 83.
[15] ibid.
[16] *Colon v Netherlands* App no 49458/06 (ECHR, 15 May 2012), [60].
[17] 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.
[18] Bart van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move* (Springer 2016), 425.
[19] Romania Constitutional Court DECISION no.12581 from 8 October 2009.
[20] Ursula Kilkelly, 'A guide to the implementation of Article 8 of the European Convention on Human Rights' (August 2003) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168007ff47> accessed 26 April 2017, p10-11.

The ECtHR in *Malone v United Kingdom*[21] observed that telephone communications data (i.e. numbers dialled) were an integral part of telephone communications data, any storage of such and release to the police without consent amounted to an interference with Article 8. In *Amann v Switzerland*, the Grand Chamber (GC) of the ECtHR reiterated that storing data relating to the "private life" of an individual falls within Article 8.[22] More specific to communications data, the ECtHR in *Copland v United Kingdom*[23] ruled that that the collection and storage of personal information relating to the applicant's telephone (numbers called, the dates and times of the calls, and their length and cost),[24] as well as to her e-mail (all e-mail activity was logged)[25] and Internet usage (websites visited, the times and dates of the visits to the websites and their duration),[26] without her knowledge, amounted to an interference with her right to respect for her private life and correspondence.[27] Specifically on data retention, the GC in *S and Marper* made it clear that 'the *mere storing* of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (author's emphasis).'[28] This is so irrespective of whether there is involvement of computer technology and expertise to make sense of said data.[29] *S and Marper* has clear applications to the detailed information revealed about individuals' private lives by communications data.[30]

This interference can be explained for several reasons. Storing information that pertains to Article 8 is not in line with the states' general negative obligations 'to *respect* human rights, which only requires states to *refrain* from interfering with the rights of individuals without sufficient justification (author's emphasis).'[31] The GC acknowledges that 'everyone has the right to live privately, away from unwanted attention'[32] and data retention would be the antithesis of this. Moreover, Bernal discusses the harm of surveillance when referring to historian Quentin Skinner[33] noting that it's the very *existence* of the system that is also harmful (author's emphasis).[34] As Solove suggests, surveillance can have problematic effects on privacy because it can create anxiety, discomfort and alter behaviour.[35] Because of its inhibitory effects, surveillance is a tool for social control,[36] whether for better or worse,

[21] *Malone v UK* App no. 8691/79 (ECHR, 2 August 1984), [84].
[22] *Amann v Swtizerland* App no. 27798/95 (ECHR, 16 February 2000), [65].
[23] *Copland v UK* App no. 62617/00 (ECHR, 3 April 2007).
[24] ibid, [10].
[25] ibid, [12].
[26] ibid, [11].
[27] Ibid, [44].
[28] *S and Marper v UK* App nos. 30562/04 and 30566/04 (ECHR, 4 December 2008), [67].
[29] ibid, [75]; Thérèse Murphy and Gearóid Ó Cuinn, 'Works in Progress: New Technologies and the European Court of Human Rights' (2010) HRLR 10:4 601, 629.
[30] Ian Brown, 'Communications Data Retention in an Evolving Internet' (2010) International Journal of Law and Information Technology 19:2 95, 103.
[31] Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) Harvard International Law Journal 56, 81, 118-119; Marko Milanovic, *Extraterritorial Application of Human Rights Treaties Law, Principles, and Policy* (Oxford University Press 2011), 209-222; Mistale Taylor, 'The EU's human rights obligations in relation to its data protection laws with extraterritorial effect' (2015) International Data Privacy Law 5:4 246, 252.
[32] *Bārbulescu v Romania* App no. 61496/08 (ECHR, 5 September 2017), [70].
[33] Quentin Skinner and Richard Marshall, 'Liberty, Liberalism and Surveillance: a historic overview' *openDemocracy* (26 July 2013) <https://www.opendemocracy.net/ourkingdom/quentin-skinner-richard-marshall/liberty-liberalism-and-surveillance-historic-overview> accessed 9 November 2017.
[34] Paul Bernal, (n4), 250.
[35] Daniel Solove, *Understanding Privacy* (Harvard University Press 2009), 108.
[36] ibid.

surveillance is harmful in all settings.[37] It is Kafkaesque because it also creates powerlessness, vulnerability, and dehumanisation created by the assembly of dossiers of personal information where individuals lack any meaningful form of participation in the collection and use of their information.[38] This dehumanisation makes no difference whether surveillance is conducted by an undercover police officer or a computer algorithm tracking ones every move.[39] This accords with the GC's position in *S and Marper* where it was noted that the storage of data *however obtained* has a *direct impact* on the private life interest of an individual's irrespective of subsequent use of said data (author's emphasis).[40] This not only rejects[41] the UK's Investigatory Powers Tribunal (IPT) reasoning[42] that genuine intrusions of Article 8 only occur when the data is 'read,' but also the sentient being argument (which the IPT's logic stems from) which notes computer sifting does not invade privacy because private data is kept from humans.[43] Bernal notes that this is the logic behind the ECtHR's reasoning in *Klass* that the mere existence of laws that *allows data gathering* produces the menace of surveillance which interferes with Article 8, *S and Marper* is the logical extension of *Klass* (author's emphasis).[44] Moreover, not only does data gathering pose harms and risks, it also creates vulnerabilities for the data (misuse, misappropriation, hacking, loss, corruption and error) the surveillance systems (intentional, accidental misuse by authorities and third parties) and function creep.[45] Bernal continues that data gathering as a matter of course regardless of innocence or guilt fits more closely with police states such as East Germany's Stasi, and Romania's Securitate.[46] Douwe Korff went further by arguing that today's capabilities are what the Stasi only could have dreamed of.[47] This is precisely why the ECtHR in *Klass* highlighted its awareness 'of the danger such as law poses of undermining or even destroying democracy on the ground of defending it.'[48]

However, this argument can be pursued further because 'the term "private life" must not be interpreted restrictively.'[49] As Ivana Roagna details, the notion of '*private life is much wider than that of privacy*, encompassing a sphere within which every individual can freely develop and fulfil their personality, both in relation to others and with the outside world (author's

---

[37] ibid, 112.
[38] Daniel Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) Standford Law Review 53 1393; Carl S. Kaflan, 'Kafkaesque? Big Brother? Finding the Right Literary Metaphor for Net Privacy' *The New York Times* (New York City, 2 February 2001) <http://www.nytimes.com/2001/02/02/technology/kafkaesque-big-brother-finding-the-right-literary-metaphor-for.html> accessed 17 January 2018.
[39] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W.W. Norton 2016), 7.
[40] *S and Marper*, (n28), [121].
[41] Matthew White, 'The Privacy International case in the IPT: respecting the right to privacy?' (14 September 2017) <https://eulawanalysis.blogspot.co.uk/2017/09/the-privacy-international-case-in-ipt.html> accessed 3 January 2018.
[42] *Privacy International v the Secretary of State for Foreign and Commonwealth Affairs and Others* [2017] IPT/15/110/CH, [19].
[43] Richard A. Posner, 'Our Domestic Intelligence Crisis' *The Washington Post* (Washington, D.C, 21 December 2005) <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html> accessed 3 January 2018.
[44] Paul Bernal, (n4), 250-1.
[45] ibid, 251.
[46] ibid, 259-260; see Chapter 1.
[47] Douwe Korff, 'We can use European law to challenge this spying' (23 June 2013) <https://www.theguardian.com/commentisfree/2013/jun/23/european-law-challenge-surveillance-human-rights> accessed 9 November 2017.
[48] *Klass*, (n13), [49].
[49] *Amann*, (n22), [65].

emphasis).'[50] The European Commission of Human Rights (ECommHR) acknowledged as much from as early as 1976.[51] It was noted in *Szabo* that:

> Given 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 protection of private life even more acutely* (author's emphasis).[52]

This statement allows for further consideration of various aspects of private life to highlight the impact of communications data retention has.

(b) Other ways in which data retention impacts on private life

ECommHR acknowledged that private life does not end at 'the right to privacy, the right to live, as far as one wishes, protected from publicity.'[53] Private life has also been acknowledged to be a 'broad term not susceptible to exhaustive definition.'[54] Private life encompasses the physical and psychological integrity of a person.[55]

i. Psychological Integrity

In *S and Marper* the applicants maintained that retention of fingerprints and DNA data would have psychological implications, especially for children. From an EU perspective, Advocate General (AG) Cruz Villalón in *Digital Rights Ireland* noted that the '*vague feeling of surveillance* created raises very acutely the question of the data retention period (author's emphasis).'[56] Rozemarijn van der Hilst noted that according to a German poll on the effects of the implementation of the Data Retention Directive, 52% said they would not use telecommunications for contact with drug counsellors, psychotherapists or marriage counsellors and 11% said they had already abstained from using phone, cell phone or email in certain occasions.[57] This is better known as the 'chilling effect' whereby 'the fear of being watched or eavesdropped upon makes people change their behaviour, even behaviour that is not illegal or immoral.'[58] Data retention may not meet the threshold[59] for affecting psychological integrity, but Moreham believes interception (which data retention is just as intrusive as (see Chapter 3)) would.[60] Moreover, Valerie Aston by implication notes that data

---

[50] Ivana Roagna, (n12), p12; Ursula Kilkelly, (n20), p11.
[51] *X v Iceland* App no. 6825/74 (ECHR, 18 May 1976).
[52] *Szabo and Vissy v Hungary* App no. 37138/14 (ECHR, 12 January 2016), [53].
[53] *X v Iceland* App no. 6825/74 (ECHR, 18 May 1976).
[54] *Aksu v Turkey* App nos. 4149/04 41029/04 (ECHR, 15 March 2012), [58].
[55] *S and Marper*, (n28), [66].
[56] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] ECR I-845, Opinion of Cruz Villalón, [72].
[57] Rozemarijn van der Hilst, 'Human Rights Risks of Selected Detection Technologies Sample Uses by Governments of Selected Detection Technologies' (2009) <http://www.detecter.bham.ac.uk/D17.1HumanRightsDetectionTechnologies.doc> accessed 26 April 2017, p20-21; German Forsa Institute, 'Meinungen der Bunderburger zur Vorratsdatanspeicherung' (28 May 2008) <http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf> accessed 26 April 2017.
[58] Rozemarijn van der Hilst, (n57), p20.
[59] Ivana Roagna, (n12), p24.
[60] Nicole Moreham, 'The right to respect for private life in the European Convention on Human Rights: a re-examination' (2008) EHRLR 1 44, 53.

retention has the potential to result in an intrusion into psychological integrity, as well as limiting personal autonomy.[61]

ii. Personal Autonomy

This chilling effect relates to autonomy, which is an important principle underlying the interpretation of the guarantees provided for by Article 8.[62] This is crucial given that 'the very essence of the Convention is respect for human dignity and human freedom.'[63] The ECtHR regards personal autonomy as 'ability to conduct one's life in a manner of one's own choosing.'[64] Personal autonomy is said to encompass a sphere in which 'everyone can freely pursue the development and fulfilment of his or her personality and to establish and develop relationships with other persons and the outside world.'[65] This principle has two aspects, personal development, and development with others. As Bernal notes:

> People use the internet to establish and support personal relationships, to find jobs, to bank, to shop, to gather the news, to decide where to go on holiday, to concerts, museums or football matches. Some use it for education and for religious observance – checking the times and dates of festivals or details of dietary rules. There are very few areas of people's lives that remain untouched by the internet.[66]

This nurtures autonomous individuals, providing them with space to develop opinions and ideas, which in turn betters' society as a whole.[67] Failure to protect the sphere of social relationships, may also lead to a failure in defending a *democratic state*[68] as privacy is important for democracy, in terms of voter autonomy and its attraction of talented people to public office (author's emphasis).[69] The ECtHR acknowledges the importance of social relationships in that private life covers the physical and *psychological integrity* of a person, the right to approach others and establish and develop relationships with other human beings (private social life)[70] and it can sometimes embrace aspects of an individual's physical and social identity (author's emphasis).[71] This also includes ethnic identity in the sense that any negative stereotyping of a group, when it reaches a certain level, is capable of impacting on the group's sense of identity and the feelings of self-worth and self-confidence of members of the group. This in turn can be seen as affecting the private life of members of the *group*,[72] raising discrimination issues (see below).

---

[61] Valerie Aston, 'State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives' (2017) EJLT 8:1 <http://ejlt.org/article/view/548/730> accessed 28 April 2017.
[62] *Aksu*, (n54), [58].
[63] *Pretty v UK* App no. 2346/02 (ECHR, 29 April 2002), [65].
[64] ibid, [62].
[65] *Jehova's witnesses of Moscow v Russia* App no. 302/02 (ECHR, 10 June 2010), [117].
[66] Paul Bernal, (n4), 247.
[67] Kirsty Hughes, 'The social value of privacy, the value of privacy to society and human rights discourse' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy Interdisciplinary Perspectives* (Cambridge University Press 2015), 229.
[68] Francesca Malloggi, 'The Value of Privacy for Social Relationships' (2017) Social Epistemology Review and Reply Collective 6:2 68, 70.
[69] Kirsty Hughes, (n67), 228-229.
[70] *Bārbulescu*, (n32), [70].
[71] *Campanelli v Italy* App no. 25358/12 (ECHR, 24 January 2017), [159].
[72] *Aksu*, (n54), [58].

Chapter 3 discussed what could be revealed from the umbrella term of communications data, it is worth just summarising that it can reveal religious, sexual preferences, political leaning[73]… *all in all, it reveals an entire life* (author's emphasis).[74] This can be based on browsing habits, to just places visited. The ECtHR firmly asserted that 'there can be no doubt that sexual orientation and activity concern an intimate aspect of private life.'[75] Although falling more firmly with the data protection aspect of Article, it has been noted that intimate data i.e. regarding health status, religious attitudes fall within Article 8.[76] Conversations with political associates also fall within the ambit of private life,[77] especially since privacy has a political value.[78] The ability to develop oneself and form relationships is increasingly done so online, and data retention interferes with all these activities. This is an early indicator of the democratic underpinning Article 8 possess.

In *Niemetz v Germany*[79] the ECtHR stressed that private life included professional and business activities as it was difficult to distinguish when an individual may be conducting business activities and when not. This is especially when business activities are of a liberal nature such as lawyers, journalists[80] and civil society organisations.[81] This, therefore, also raises issues (but not limited to) of legal professional privilege, the protection of journalistic sources and monitoring the very organisations that seek to challenge said surveillance laws.

iii. Anonymity

The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye noted that broad mandatory data retention policies limit an individual's ability to remain anonymous. [82] Kaye continues that requiring Internet services and telecommunications providers to retain data results in the state by proxy having everyone's digital footprint.

The right to anonymity is not (as of yet) an explicit principle found within Article 8, but it will be argued that it is an inherent feature and is consistent with respecting private life. This can be seen in in *Rotaru v Romania*, where the GC rejected Romania's argument that engaging in political activities acted as a waiver to anonymity[83] by agreeing there was an interference with Article 8.[84] The Budapest Convention and the Council of Europe's Declaration on Freedom of Communication on the Internet regard anonymity (and encryption) as a legitimate principle in protecting privacy, protection against online surveillance and to enhance freedom of

---

[73] Paul Bernal, (n4), p253.
[74] Kai Biermann, 'Betrayed by our own data' (10 March 2011) <http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz> accessed 13 April 2017.
[75] *Laskey, Jaggard and Brown v UK* App nos. 21627/93 21826/93 21974/93 (ECHR, 19 February 1997), [36].
[76] *Magyar Helsinki Bizottsag v Hungary* App no. 18030/11 (ECHR, 8 November 2016), [192]. See sections 4.6(f) and 4.9 here.
[77] Nicole Moreham, (n60), 61.
[78] Benjamin J. Goold, 'Surveillance and the Political Value of Privacy' (2009) Amsterdam Law Forum 3 1:4.
[79] *Niemetz v Germany* App no. 13710/88 (ECHR, 16 December 1992), [29].
[80] *Ernst and Others v Belgium* App no. 33400/96 (ECHR, 15 July 2003), [110].
[81] *Liberty and Others v UK* App no. 58243/00 (ECHR, 1 July 2008), [56].
[82] David Kaye, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (22 May 2015) Human Rights Council, U.N. Doc.A/HRC/29/32 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement> accessed 28 April 2017, para 55.
[83] *Rotaru v Romania* App no. 28341/95 (ECHR, 4 May 2000), [42].
[84] ibid, [46].

expression.[85] This link between anonymity and privacy was also observed by Catalina Botero of the Inter-American Commission on Human Rights,[86] with both the Canadian Supreme Court[87] and US courts recognising the importance of anonymity. Anonymity forms the basis of Patrick Breyer's challenge against German data retention laws.[88] In *Delfi AS v Estonia* the GC acknowledged that anonymity is capable of promoting the free flow of ideas and information in an important manner, including, notably, on the Internet.[89] However, it was also noted how the dissemination can aggravate the effects of unlawful speech.[90] The GC did acknowledge that individuals may only be traceable, to a limited extent, through the information retained by Internet access providers.[91] This, however, does not take into account that data retention obligations do not just fall on squarely on ISPs (as David Kaye notes above), but many other service providers as will be discussed.[92] When the GC acknowledged that anonymity is an important value[93] on the Internet, this was done without bearing in mind the wide extent at which data can be retained, and who can be obligated to retain. This would only serve to highlight the greater importance of the value of anonymity.

Chapter 3 noted that under Part 4 of the IPA 2016, Virtual Private Networks (VPNs) could be compelled to generate data possibly revealing browsing habits, thus destroying anonymity. Privacy International's General Counsel, Caroline Wilson Palow noted concerns about anonymity regarding Internet Connection Records (ICRs).[94] Palow noted that if ICRs revealed that someone visited crimestoppers-uk.org – an anonymous tips website designed to solve crimes, who put in that tip could easily be figured out. Palow concluded that destroying anonymity could undermine the ability to solve crime. Support for Palow's claims come from Jennifer Cole and Alexandra Stickings who note that independent research conducted by UK charity Crimestoppers highlighted that 95% of those that contacted the organisation would *not* have gone directly to the police (author's emphasis).[95] This could be for many reasons including anonymous reporting being less intimidating than a face-to-face,[96] feelings of vulnerability to crime, not necessarily being a law abiding citizen themselves or fear of reprisals for reporting a crime.[97] On destroying anonymity, Cole and Alexandra note that digital traces (such as phone number, IP Address and geolocation)[98]recorded by technology (such as

[85] Budapest Convention on Cybercrime, Article 2, Explanatory Report, para 62; Declaration on Freedom of Communication on the Internet, Principle 7.
[86] Catalina Botero, Inter-American Commission on Human Rights, 'Freedom of Expression on the Internet' (2013) <https://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf> accessed 1 May 2017, para 23.
[87] *R v Spencer* [2014] 2 SCR 212, [48], [50], [62], [66]; *Awtry v Glassdoor* Case No. 16-mc-80028-JCS,
[88] *Breyer v Germany* App no. 50001/12 Communicated on 21 March 2016; Written submissions (5 September 2016) <https://www.article19.org/data/files/medialibrary/38485/Breyer-v-Germany---App.-No.-50001-12.pdf> accessed 29 April 2017.
[89] *Delfi AS v Estonia* App no. 64569/09 (ECHR, 16 June 2015), [147].
[90] ibid.
[91] ibid, [148].
[92] See Chapter 6.
[93] *Delfi AS*, (n89), [149].
[94] Joint Committee on the Draft Investigatory Powers Bill, *oral evidence*, <https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf> accessed 29 April 2017, Caroline Wilson Palow, answer to Q130.
[95] Jennifer Cole and Alexandra Stickings, 'The Future of Crime Reporting' (2017) The RUSI Journal 162:1 68, 69.
[96] ibid, 71; Adam N. Johnson, 'Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity' (2001) European Journal of Social Psychology 31 177.
[97] Jennifer Cole and Alexandra Stickings, (n95), 70.
[98] ibid, 72.

the ISP or the reporting system itself)[99] for reporting crimes 'now make it easier than ever to trace a report back to the person who made it.'[100] Crimestoppers specifically withholds communications data from the police when passing on reports.[101] As Cole and Alexandra highlight, communications data are often captured automatically and its separation inside the reporting system is likely to be extremely important if it is to offer the perception and reassurance of relative anonymity in the context of witness protection.[102] Additionally they note (using an example) that although Crimestoppers reports are inadmissible in court, without leads for police to follow, convictions may not be possible.[103]

David Kaye also noted that:

> Encryption and anonymity, today's leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression.[104]

Linking with freedom of expression, Lord Neuberger in the UK noted that in the context of anonymous speech, an author's Article 8 rights reinforces their Article 10 rights.[105] Neuberger continued that in this context, Article 8 rights are of *fundamental importance* (author's emphasis).[106]

Anonymity must yield *on occasion* to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others (author's emphasis).[107] However, the general nature of retention powers as Breyer notes interferes with anonymity[108] (by even impeding or eliminating it)[109] on a scale that cannot be compared to *KU v Finland*[110] which concerned the anonymity of an *individual.* Finland were found to be in violation of Article 8 because national law could not compel ISP's to provide the identity of a person who placed an advertisement of a minor online. Notably, the ECtHR held that on *occasion,* Article 8 and 10 must yield to other legitimate imperatives such as the prevention of disorder/crime (author's emphasis).[111] This was seized upon by the Home Office to justify blanket indiscriminate data retention as envisaged in the draft Communications Data Bill.[112] Breyer also notes (in reference to *Rotaru*) that anonymity has been traditionally linked to the protection

---

[99] ibid, 72.
[100] ibid, 69.
[101] ibid, 72.
[102] ibid, 75.
[103] ibid, 70-71.
[104] David Kaye, (n82), para 1.
[105] Lord Neuberger, '"What's in a name?" - Privacy and anonymous speech on the Internet' (30 September 2014) <https://www.supremecourt.uk/docs/speech-140930.pdf> accessed 29 April 2017, para 25.
[106] ibid, para 42.
[107] *Delfi AS*, (n89), [149].
[108] *Breyer*, (n88), para 24.
[109] Lilian Mitrou, 'Communications Data Retention: A Pandora's Box for Rights and Liberties?' in Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis, and Sabrina di Vimercati (ed) *Digital Privacy: Theory, Technologies, and Practices* (Auerbach Publications 2007), 426.
[110] *KU v Finland* App no. 2872/02 (ECHR, 2 December 2008).
[111] ibid, [49].
[112] Home Office, *Draft Communications Data Bill* (Cm 8359, 2012), 97.

of personal data.[113] Since truly anonymous data is not personal data and so not a data protection issue. Recital 26 of Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR) notes that anonymous data is not personal data and therefore does not apply to it. However, in light of Big Data, achieving anonymity is meaningless as it serves 'little more than fig leaves to hide the actually easy reidentifiability of the data.'[114] Re-identification is possible through the cross-referencing of anonymous data,[115] moreover, anonymity is no safeguard against the possibility of characterising individuals' behaviour or forecasting future behaviours.[116] Therefore, the distinction between personal data and anonymous data is no longer clear.[117]

iv. Data Protection

Another aspect of private life protection derives from personal data regulation. The ECtHR has been willing to accept a number of the notions essential to the right to data protection under the scope of the Convention.[118] In *S and Marper* the GC noted that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private…life.[119] The European Data Protection Supervisor (EDPS) noted that the protection of personal data ensures a person's right to respect for private life, freedom of expression and association[120] (which links to section 4.5/6). Personal data has been defined as 'any information relating to an identified or identifiable individual.'[121] The GC continued that domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of Article 8.[122] This includes[123] consistency with Articles 5 (quality of data),[124] 6 (special categories of data)[125] and 7 (data security)[126] of the Convention of 1981.[127] The GC also considered the relevance of Committee of Ministers Recommendation No. R (87)

---

[113] *Breyer*, (n88), para 5.
[114] Douwe Korff, 'Passenger Name Records, data mining & data protection: the need for strong safeguards' (15 June 2015) <https://rm.coe.int/16806a601b> accessed 6 November 2017, p36.
[115] Antoinette Rouvroy, '"Of Data and Men" - Fundamental rights and freedoms in a world of Big Data' (11 January 2016) <https://rm.coe.int/16806a6020> accessed 6 November 2017, 20-21.
[116] ibid, 22.
[117] ibid, 20.
[118] Bart van der Sloot, 'Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?' (2014) JIPITEC 5:3, 233, para 17.
[119] *S and Marper* (n28), [103].
[120] Opinion 8/2016 'EDPS Opinion on coherent enforcement of fundamental rights in the age of big data' (23 September 2016) <https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf> accessed 13 November 2017, p7.
[121] Article 4(1) of the Regulation (EU) 2016/679, the General Data Protection Regulation and Article 2(a) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series no. 108, Strasbourg, 1981.
[122] *S and Marper* (n28), [103].
[123] *Z v Finland* App no. 22009/93 (ECHR, 25 February 1997), [95].
[124] Obtained and processed fairly and lawfully; stored for specified and legitimate purposes and not used in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are stored; accurate and, where necessary, kept up to date; preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.
[125] Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.
[126] Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.
[127] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series no. 108, Strasbourg, 1981.

15 on the use of personal data in the police sector[128] Both the provisions and principles of Convention of 1981 and Recommendation No. R (87) 15 are of some importance when considering safeguards.[129] The GC highlighted that need for safeguards is all the greater where personal data is undergoing *automatic processing* (exasperated by ever greater frequency of privacy invasive technologies which may affect social life more generally)[130], not least when such data are used for police purposes (author's emphasis).[131] Moreover, national law should ensure that such data are *relevant and not excessive in relation to the purposes for which they are stored*, preserved in a form which permits identification of the data subjects for *no longer than is required for the purpose for which those data are stored* (author's emphasis).[132] Additionally, the GC maintained that adequate guarantees must be in place so that retained personal data were efficiently protected from misuse and abuse, *especially* concerning protection of special categories of more sensitive data (author's emphasis).[133] These sensitive personal data includes data revealing racial origin, political opinions or religious or other beliefs, health or sexual life. This, therefore, displays the interlink between various aspects of private life where data protection has a connection with anonymity and the various aspects of autonomy i.e. social identity etc. The GC in *S and Marper* noted that '[w]here a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted.'[134] As Bart van der Sloot notes, autonomy and informational self-determination have been accepted as core rationales underlying Article 8 ECHR in cases regarding the processing of personal data,[135] thus sharing similarities with German Basic Law.[136] This point becomes important considering Facebook (albeit in Australia and New Zealand) has been accused[137] (but denies)[138] of exploiting young user's data by helping advertisers target teens who felt 'worthless.' This is important as Aral Balkan argues that new technologies should be looked at as extensions of *ourselves*.[139]

EU texts are also of importance, the ECtHR referred to Article 8 (right to the protection of personal data) of the CFR,[140] the (replaced) Directive 95/46/EC, Data Protection Directive (DPD) and GDPR.[141] This is important given that the ECtHR's expansive recourse to external

[128] *S and Marper* (n28), [42].
[129] *MM v UK* App no. 24029/07 (ECHR, 13 November 2012), [196]
[130] Beate Roessler and Dorota Mokrosinska 'Introduction' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy Interdisciplinary Perspectives* (Cambridge University Press 2015), 2.
[131] *S and Marper* (n28), [103].
[132] ibid.
[133] ibid.
[134] ibid, [102].
[135] Bart van der Sloot, (n118), 234, para 19; See *Satakunnan Markkinapörssi Oy and Satamedia Oy v v Finland* App no. 931/13 (ECHR, 27 June 2017), [137]; *Malone*, (n21), Concurring Opinion of Judge Petitti; *Youth Initiative for Human Rights v Serbia* App no. (ECHR, 25 June 2013), Joint Concurring Opinions of Judges Sajó and Vučinić, [3].
[136] 'Population Census Decision', Judgment of 15 December 1983, 1 BvR 209/83, BVerfGE 65, 1; Article 1(1) and 2(1) German Basic Law.
[137] Sam Machkovech, 'Report: Facebook helped advertisers target teens who feel "worthless"' *Ars Technica* (1 May 2017) <https://arstechnica.com/business/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless/> accessed 2 May 2017.
[138] Comments on Research and Ad Targeting <https://newsroom.fb.com/news/h/comments-on-research-and-ad-targeting/> accessed 2 May 2017.
[139] Aral Balkan, 'The nature of the self in the digital age' (3 March 2016) <https://ar.al/notes/the-nature-of-the-self-in-the-digital-age/> accessed 13 November 2017.
[140] *MM*, (n129), [144].
[141] *Surikov v Ukraine* App no. 42788/06 (ECHR, 26 January 2017), [57-8].

rules of international law[142] because it can inform the ECtHR's reasoning.[143] The GDPR also interlinks with the ECHR in that Article 88(2) refers to safeguarding the data subjects *human dignity*, which is the very essence of the ECHR. The European Data Protection Supervisor (EDPS) explains further that better respect for and safeguarding of human dignity could counterweigh the pervasive surveillance and power asymmetry which now confronts individuals. The EDPS continued that the ECHR is the starting point with regards to the inviolability of human dignity, which is fundamental for a collection of rights including privacy and data protection, hence the introduction of Convention 108 and subsequent data protection regimes to deal with potential for the erosion of privacy and dignity through large scale personal data processing.[144]

Data protection (Article 8 CFR) has been argued to extend[145] beyond 'privacy.'[146] It has been argued that data protection promotes informational self-determination which flows from the individual's right to personality and redresses detrimental power and information asymmetries between data subjects and those that process their personal data.[147] It has also been noted that data protection extends beyond privacy because processing of personal data must be done fairly and for a specified purpose.[148] However, privacy is a much broader concept,[149] it was previously noted above that private life relates to autonomy, informational self-determination amongst others aspects. Moreover, Lilian Edwards noted that the European data protection system had in practice been less than satisfactory which intensified with the Internet as the direct marketing medium highlighted dismaying gaps in the system.[150] Tijmen Wisman highlights that in the age of the Internet of Things 'when data leave[s] the exclusive control of the individual, this data might be protected according to the law, but still there will be a breach of privacy.'[151] This lack of control intensifies in light of Big Data.[152] One thing is certain however, data protection and privacy do not protect the exact same interests.[153] Moreover, on the specifics of data retention, data protection is argued to provide insufficient protection

[142] Julian Arato, 'Constitutional Transformation in the ECtHR: Strasbourg's Expansive Recourse to External Rules of International Law' (2012) Brooklyn Journal of International Law 37:2.
[143] *Hirst v UK* App no. 74025/01 (ECHR, 6 October 2005), [35-37]; Kanstantsin Dzehtsiarou, 'Comparative Law in the Reasoning of the European Court of Human Rights' (2010) University College Dublin Law Review 10 109; Eirik Bjorge, 'National supreme courts and the development of ECHR rights' (2011) Int J Const Law 9:1 5.
[144] European Data Protection Supervisor, 'Opinion 4/2015 Towards a New Digital Ethics Data, Dignity and Technology' <https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf> accessed 19 May 2017, p12; Luciano Floridi, 'On Human Dignity as a Foundation for the Right to Privacy' (2016) Philosophy & Technology 29:4.
[145] Orla Lynskey, 'Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order' (2014) ICLQ 63:3 569.
[146] Note that as stated above, 'private life' extends *beyond* 'privacy' and therefore, the premise of this assertion becomes questionable.
[147] Orla Lynskey, (n145), 595.
[148] Juliane Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) International Data Privacy Law 3:4 222, 225.
[149] Maria Tzanou, 'Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures' (2013) Journal of Internet Law 17:3 20.
[150] See also Lilian Edwards, 'Reconstructing Consumer Privacy Protection On-line: A Modest Proposal' (2007) International Review of Law, Computers & Technology 18:3 313, 320.
[151] Tijmen Wisman, 'Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things' (2013) EJLT 4:2 <http://ejlt.org/article/view/192/379> accessed 2 May 2017.
[152] Bart van der Sloot, 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) International Data Privacy Law 4:4 307; Manon Oostveen, 'Identifiability and the applicability of data protection to big data' (2016) International Data Privacy Law 0:0 1.
[153] Juliane Kokott and Christoph Sobotta, (n148); Maria Tzanou, (n149).

because it negates the protective effects of most of the eight Data Protection Principles and is susceptible to function creep (future undefined purposes).[154] Any breach of Article 8 should be enforced.[155] Nor is the ICO a powerful regulator[156] which may raise adequate safeguard issues with Article 8. Whether data protection or right to respect for private life provides greater protection is beyond the scope of this thesis, but it is important to remember that the GC in *S and Marper* noted that the protection of personal data is of *fundamental importance*, not only to private, but family life[157] also (author's emphasis). This not only implies that every aspect of personal data is now within the scope of private life, it leads to a discussion on another aspect of Article 8, that of family life.

4.3 Family life

Similar to the notion of private life, family life is also a loose concept. [158]Relationships that have been found to be covered by family life includes biological and non-biological relationships.[159] The 'mutual enjoyment by members of a family of each other's company constitutes a fundamental element of family life.' [160] Baroness Hale in *Countryside Alliance*[161] went further and highlighted that Article 8 reflects two separate fundamental values, one being the inviolability of personal and psychological space where individuals develop their own sense of self and relationships with others. Hale continued that this is 'fundamentally what families are for and why democracies value family life so highly' as they 'nurture individuality and difference'[162] something that totalitarian regimes seek to subvert.

The importance of family life becomes more profound in the digital era where it has been suggested that social media could strengthen family bonds, reunite improve family relationships and personal development.[163] Raelene Wilding demonstrated that 'the desire to communicate across distance was nevertheless common to all the families' describing them as 'transnational families.'[164] Wilding continued that the lack of face-to-face contact sometimes 'made the relationship feel so much more intimately connected.'[165] In 2013, Microsoft demonstrated that one in three families use technology to communicate *within* the home

[154] Chris Pounder, 'Nine principles for assessing whether privacy is protected in a surveillance society' (2008) Identity Journal Limited 1:1 1, 5.
[155] Chris Pounder, 'Is the NHS ransomware incident a reportable data loss?' (14 May 2017) <http://amberhawk.typepad.com/amberhawk/> accessed 19 May 2017.
[156] Chris Pounder, (n154), 6.
[157] *S and Marper*, (n28), [103].
[158] *X, Y and Z v UK* App no. 21830/93 (ECHR, 22 April 1997), [36].
[159] Ivana Roagna, (n12), p28.
[160] *El-Masri v The Former Yugoslav Republic of Macedonia* App no. 39630/09 (ECHR, 13 December 2012), [248].
[161] *Countryside Alliance v and others, R (on the application of) v Attorney General & Anor* [2007] UKHL 52, [116].
[162] ibid.
[163] Amanda L. Williams and Michael J. Merten, 'iFamily: Internet and Social Media Technology in the Family Context' (2011) Family & Consumer Sciences Research Journal 40:2 150, 167; Sandra Wachter, 'Privacy: Primus Inter Pares Privacy as a precondition for self-development, personal fulfilment and the free enjoyment of fundamental human rights' (2017) Oxford Internet Institute < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903514 > accessed 1 December 2017, p21-22; Anne Stych, 'Social media reunites families after Harvey' (30 August 2017) <https://www.bizjournals.com/bizwomen/news/latest-news/2017/08/social-media-reunites-families-after-harvey.html?page=all> accessed 6 June 2018.
[164] Raelene Wilding, ''Virtual' intimacies? Families communicating across transnational contexts' (2006) Global Networks 6:2 125, 137.
[165] ibid, 139.

(author's emphasis).[166] Family members communicating with each other leads to the necessary discussion on correspondence.

4.4 Correspondence

Correspondence aims to protect the confidentiality of private communications, which has also been interpreted as guaranteeing the right to uninterrupted and uncensored communications with others.[167]

As traditional ideas of correspondence evolve, the ECtHR's jurisprudence evolves also. This was affirmed in *Copland v United Kingdom*.[168] The ECtHR held that the monitoring of telephone calls which consisted of analysis 'of the college telephone bills showing telephone numbers called, the dates and times of the calls and their length and cost' the 'web sites visited, the times and dates of the visits to the web sites' and the 'analysis of e-mail addresses and dates and times at which e-mails were sent' amounted to an interference with private life and *correspondence* within the meaning of Article 8.[169] The ECtHR acknowledged that Article 8 protects the confidentiality of private communications and the confidentiality of *all* the exchanges in which individuals may engage for the purposes of communication (author's emphasis).[170] Although correspondence applies to all communications, there are notable examples of privileged communications that are more important, including correspondence with lawyers (which may have Article 6 implications, discussed below),[171] medical profession,[172] Members of Parliament,[173]and as mentioned above numerous times correspondence with journalists. Just as Solove notes, who one may contact may be more important to the individual than what was actually communicated.[174] In acknowledging that correspondence is interfered with irrespective of the contents of a communication,[175] the ECtHR has extended protection to the means or method of communication.[176]

This highlights links between private life and correspondence in terms of the anonymity of journalistic sources and also the professional activities of the journalist. The ECtHR noted the impact upon professional activities:

> [T]he right of journalists not to disclose their sources cannot be considered a mere privilege to be granted or taken away depending on the lawfulness or unlawfulness of their sources, but is part and parcel of the right to information, to be treated with the utmost caution.[177]

---

[166] Tim Lumb, 'New Microsoft research: technology and the home' (28 October 2013) <https://www.marketingsociety.com/the-library/new-microsoft-research-technology-and-home> accessed 8 November 2017.
[167] Ivana Roagna, (n12), p32.
[168] *Copland v United Kingdom*, (n23), [10-13].
[169] ibid, [44].
[170] *Michaud v France* App no. 12323/11 (ECHR, 6 December 2012), [90].
[171] *Petrov v Bulgaria* App no. 15197/02 (ECHR, 22 May 2008), [43].
[172] *Szuluk v UK* App no. 36936/05 (ECHR, 2 June 2009), [39].
[173] ibid, [53].
[174] Daniel Solove, (n35), 68; Daniel Solove, 'Reconstructing Electronic Surveillance Law' (2004) 72 The George Washington Law Review 1701, 1728.
[175] *A v France* App no. 14838/89 (ECHR, 23 November 1993), [34-7];
[176] Ivana Roagna, (n12), p33.
[177] *Tillack v Belgium* App no. 20477/05 (ECHR, 27 November 2007), [65].

Protection of journalistic sources is vital for democratic societies as without protection, the ability to provide accurate and reliable information may be undermined.[178] Data retention poses unique challenges[179] to the protection of journalists (and other professions) discussed below.

4.5 Data retention: A Fundamental Rights Issue

In the *Belgian Linguistic Case* the ECtHR noted that the ECHR must be read as a whole, and as a consequence, a matter specifically dealt with by one provision may be regulated by other provisions of the ECtHR.[180] Benjamin J Goold noted, '[i]t is hard to imagine, for example, being able to enjoy freedom of expression, freedom of association, or freedom of religion without an accompanying right to privacy.'[181] The same sentiments are true in the communications data context.[182]

The following sections considers rights other than Article 8, but it is Article 8 which links and underpins them. This includes Articles 9 (religion, thought and conscience), 10 (expression), 11 (association), 14 (non-discrimination), 6 (fair trial) and Article 2 of Protocol 4 (free movement). Similar rights are provided for by the CFR, thus bringing in an EU element which was recognised by the European Parliament as *cornerstones of democracy*; whereas mass surveillance was incompatible with (author's emphasis).[183]

The then Interception of Communications Commissioner (IoCC) in the UK criticised public authorities and designated persons for focusing primarily on Article 8 and not giving due consideration to Article 10.[184] It is therefore necessary to now consider Article 10 ECHR.

4.6 Freedom of Expression and Article 10

> Privacy is not the enemy of freedom of speech, it is its closest ally.[185]

The then Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue commented on interrelation between privacy and freedom of expression. He contended that the right to privacy is often understood as an *essential* requirement for the realisation of the right to freedom of expression and any undue interference

---

[178] *Sanoma Uitgevers B.V. v the Netherlands* App no. 38224/03 (ECHR, 14 September 2010), [89].
[179] Sal Humphreys and Melissa de Zwart, 'Data retention, journalist freedoms and whistleblowers' (2017) Media International Australia 165:1 103.
[180] *Belgian Linguistic Case* (No.2) App nos. 1474/62, 1677/62, 1691/62, 1769/63, 1994/63, 2126/64 (ECHR, 23 July 1968), [7].
[181] Benjamin J. Goold, (n78), 4.
[182] Committee on Civil Liberties, Justice and Home Affairs, 'Text of the compromise amendments' <https://drive.google.com/file/d/0Byeaj8v2GIOacnVwVlhqMWdUWFU/view> accessed 12 November 2017.
[183] European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)) <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230> accessed 3 May 2017.
[184] Interception of Communications Commissioner 'IOCCO inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources' (4 February 2015) <http://www.iocco-uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf> accessed 6 April 2017, para 8.6.
[185] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge Intellectual Property and Information Law 2014), 52.

with privacy can both directly and indirectly limit the free development and exchange of ideas.[186] Although this freedom of expression especially on the internet can pose risks to private life[187] (such as tarnishing reputation)[188] the latter can enhance the former. It is important to consider whether data retention interferes with freedom of expression.

(a) Does Data Retention interfere with Freedom of Expression?

In *Digital Rights Ireland*, the Court of Justice of the European Union (CJEU) was asked whether Directive 2006/24, the Data Retention Directive (DRD) was compatible with the right to freedom of expression laid down in Article 11 of the Charter and Article 10 ECHR.[189] The CJEU did acknowledge that data retention raises questions relating to freedom of expression[190] and felt that it was not inconceivable that data retention may have an effect on the exercise of that right.[191] Ultimately, the CJEU felt it was unnecessary to examine data retention in light of Article 11,[192] and thus went no further. In *Tele2 and Watson*, however, the CJEU did this time find that blanket indiscriminate data retention of all data, of all persons, of all communications would be incompatible with Article 11 (including Article 7, 8 and 52(1) of the CFR).[193] The CJEU noted that:

> [T]he retention of traffic and location data could nonetheless *have an effect on the use of means of electronic communication* and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter (author's emphasis).[194]

If one considers the approach in *Klass*, the ECtHR noted that the *mere existence* of secret surveillance laws threatened the *freedom of communication* between users of telecommunications services, interference is, established. The CJEU did not explain why Article 11 CFR was interfered with, thus it is important to consider Article 10 ECHR and to ascertain *why* data retention interferes with freedom of expression in various ways.

(b) Article 10 ECHR

Article 10(1) provides that:

> Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

---

[186] Frank La Rue, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (17 April 2013) <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf> accessed 3 May 2017, para 24; Paul Bernal, (n4), 254-255.
[187] *Delfi AS*, (n89), [133].
[188] European Court of Human Rights Factsheet – 'Protection of Reputation' (October 2017) http://www.echr.coe.int/Documents/FS_Reputation_ENG.pdf> accessed 8 November 2017.
[189] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECR I-238, [18].
[190] ibid, [25].
[191] ibid, [28].
[192] ibid, [70].
[193] Joined Cases C‑203/15 and C‑698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-970, [134].
[194] ibid, [101].

Given that Article 11 CFR is Article 10 ECHR's equivalent, under Article 52(3), it will be given the same scope and meaning. The ECtHR has previously held that Article 10 applies to communications via the Internet,[195] irrespective of the type of message conveyed[196] and irrespective of whether it is commercial in nature.[197] In *Delfi*, the GC acknowledged previous case law in agreeing that 'user-generated expressive activity on the Internet provides an *unprecedented platform* for the exercise of freedom of expression.'[198] Moreover, it has been stressed that 'freedom of expression constitutes *one of the essential foundations of a democratic society* and *one of the basic conditions for its progress and for each individual's self-fulfilment* (author's emphasis).'[199] This relates to privacy, and Article 8 in two respects, one, in that Article 8 and Article 10 are foundations of democracy, and two, self-fulfilment is inextricably linked to the notion of autonomy where one 'can freely pursue the development and fulfilment of his personality.'[200] Crucially, the ECtHR has acknowledged that the *storage* of personal data related to *political opinion* engages Article 10 due to the adverse effects (see discussions on chilling effects)[201] caused by storage *without* any concrete proof of actual harm (author's emphasis).[202] This, also relates to the data protection aspect of private and family life because it involves the processing of data pertaining to political opinions/affiliations. This, therefore, as suggested above, meets the *Klass* approach of interfering with the *freedom of communication* under Article 8 must be applied *mutatis mutandis* to Article 10[203] and thus requires justification.

(c) Autonomy and Development and Fulfilment

Chapter 3 noted that privacy is important for ideas that are unconnected to democratic functions which are connected to broader autonomy based arguments for freedom of speech and intellectual development.[204] Freedom of expression (including artistic expression) is important for the development and manifestation of individuals' identities in society.[205] The ECtHR have agreed, noting that freedom of expression is essential for each individual's (and for a family)[206] self-fulfilment.[207] This relates to other aspects of private life, notably the development and embracing of physical, social and ethnic identities, interlinking Article 8 and 10.

(d) Information and Ideas

---

[195] *Ashby Donald and Others v France* App no. 36769/08 (ECHR, 10 January 2013), [34].
[196] *Groppera Radio AG and others v Switzerland* App no. 10890/84 (ECHR, 28 March 1990), [55].
[197] *Autronic AG v Switzerland* App no. 12726/87 (ECHR, 22 May 1990), [47].
[198] *Delfi AS*, (n89), [110].
[199] *Animal Defenders International v UK* App no. 48876/08 (ECHR, 22 April 2013), [100].
[200] *Gough v UK* App no. 49327/11 (ECHR, 28 October 2014), [182]; Sandra Wachter, (n163), p21-22.
[201] See sections 4.1(b)(i)/(ii), 4.5(e)/(f)/(g), 4.6(d), 4.7(f), 4.9(e) and 4.11.
[202] *Segerstedt-Wiberg and Others v Sweden* App no. 62332/00 (ECHR, 6 June 2006), [107].
[203] *Weber and Saravia v Germany* App no. 54934/00 (ECHR, 29 June 2006), [145]. This case was in the context of journalism, but as *Sergerstedt-Wiberg and Others* have demonstrated, being a journalist is not a necessary preresiquite for interference with Article 10.
[204] Kirsty Hughes, (n67), 229.
[205] Council of the European Union, 'EU Human Rights Guidelines on Freedom of Expression Online and Offline' (12 May 2014) <https://eeas.europa.eu/sites/eeas/files/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf> accessed 3 May 2017, para 3.
[206] See section 4.2.
[207] *Satakunnan Markkinapörssi Oy and Satamedia Oy*, (n135), [124].

Article 10 is applicable not only to information or ideas that are favourably received, inoffensive or indifferent, but to those that offend, shock and disturb, without such pluralism, tolerance and broadmindedness there can be no 'democratic society.'[208]

It is important to allow space to develop opinions and ideas to benefit society.[209] In a successfully developing society all of its members contribute by means of their talents, energy and intellect.[210] This all requires the *communication* of ideas, and the *freedom* to do so. As Solove suggests, anonymity or the use of pseudonyms, both of which has allowed freedom of expression to flourish, protects those who read or listen to unpopular ideas.[211]

(e) Anonymity, Whistleblowing and Journalism

Anonymity was discussed at length in section 4.2(b)(3). It is worth repeating, however, what Lord Neuberger[212]articulated, in that in the context of anonymous speech, an author's Article 8 rights *reinforces* their Article 10 rights (because it amongst other things, grants anonymity), in which Article 8 rights become of *fundamental importance*.[213] Moreover, Frank La Rue in 2013 argued that anonymity of communications is one of the most important advances enabled by the Internet, allowing individuals to express themselves freely without fear of retribution or condemnation. [214] La Rue continued that restrictions on anonymity can have a chilling effect, which dissuades the free expression of information and ideas.[215] This can also result in individuals' de facto exclusion from vital social spheres, undermining their rights to expression and information, and exacerbating social inequalities,[216] such as direct and indirect censorship due to China's Twitter-like 'Weibo' which introduced real-name registration.[217] Additionally, it can have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimisation.[218] This raises private life aspects such as autonomy, physical and psychological integrity.

As Bernal maintains, strong anonymity is needed for whistleblowers.[219] David Wilson[220] stressed the importance of why whistleblowers need anonymity, where he detailed whistle blowing which lead to his unemployment and affected his employment prospects.[221] Such issues can both fall within the ambit of Article 8 and 10[222] as the latter includes 'the freedom to impart information.'[223]

---

[208] *Animal Defenders International*. (n199), [100].
[209] Kirsty Hughes, (n67), 229.
[210] *Campanelli*, (n71).
[211] Daniel Solove, (n35), 125.
[212] Lord Neuberger, (n105), para 25.
[213] ibid, para 42.
[214] Frank La Rue, (n186), para 23.
[215] ibid, para 49.
[216] ibid.
[217] Lord Neuberger, (n105), para 26.
[218] Frank La Rue, (n186), para 24. For example, a trafficking victim being subject to criminal proceedings.
[219] Paul Bernal, (n185), 238-9.
[220] Co-founder of War Child, a charity set up to help child victims of war in former Yugoslavia.
[221] David Wilson, 'I exposed corruption at War Child. Here's why whistleblowers need anonymity' *The Guardian* (London, 10 April 2017) <https://www.theguardian.com/voluntary-sector-network/2017/apr/10/whistleblower-war-child-need-anonymity-corruption> accessed 5 May 2017.
[222] Michael Ford, 'Article 8: Right to respect for private and family life (The implications on unfair dismissal)' (7 November 2014) <http://www.ier.org.uk/blog/article-8-right-respect-private-and-family-life-implications-unfair-dismissal> accessed 5 May 2017.
[223] *Guja v Moldova* App no. 14277/04 (ECHR, 12 February 2008), [53], [55].

Wilson noted that his whistleblowing only gained traction once he went to the press.[224] It is therefore important to discuss the press, journalism, whistle blowing and data retention in relation to Article 10. Journalism is regarded as the 'fourth estate'[225] (a segment of society having significant influence on society outside of the political system) in which political reporting and investigative journalism attract a high level of protection under Article 10.[226] Protections, however, are uniquely challenged in the context of data retention.[227] A study by the World Association of Newspapers and News Publishers (WAN-IFRA) on behalf of the United Nations Educational, Scientific and Cultural Organization (UNESCO) highlighted that legal source protection was jeopardised by mandatory data retention laws because of the risk of exposing sources.[228] Another key finding was that without substantial limitations and protections of data retention, investigative journalism that relies on confidential sources will be difficult to sustain and reporting in many other cases will encounter inhibitions on part of potential sources.[229] Even when journalists encrypt content they may neglect the metadata, leaving behind digital breadcrumbs when they communicate with their sources, making it easy to identify sources with insufficient or non-existent safeguards.[230] It was also noted that the chilling effect on confidential sources is further exacerbated given the risk of profiling and exposure by the combinations of data retention and Big Data analysis.[231] The UK has dropped to 40th place in the World Press Freedom Index, citing the IPA 2016 as having 'insufficient protection mechanisms for whistleblowers, journalists, and their sources, posing a serious threat to investigative journalism.'[232] Given the revealing nature of communications data, journalists could unwittingly disclose their sources by virtue of the fact that communications between them and whistleblower is retained. Maintaining the confidentiality of sources is not a mere privilege dependent upon the lawfulness of their sources, but is a part to the right to information, which is to be treated with utmost caution.[233] This not only compromises the professional activities protected under private life, it also interferes with the correspondence of both journalist and source. Another aspect of whistleblowing is the fact that concerns disclosed by whistleblowers can cross national boundaries, affecting members of the public in more than one country and requiring a response by regulators and governments in multiple States, particularly where the worker operates in an industry that is globalised and operates transnationally.[234] This warrants the discussion of the 'regardless of frontiers' aspect of Article 10.

(f) Regardless of Frontiers

[224] David Wilson, (n221).
[225] Sal Humphreys and Melissa de Zwart, (n179).
[226] *Mosely v UK* App no. 48009/08 (ECHR, 10 May 2011), [129].
[227] Sal Humphreys and Melissa de Zwart, (n179).
[228] Julie Posetti, 'Protecting Journalism Sources in the Digital Age' (2017) <http://unesdoc.unesco.org/images/0024/002480/248054E.pdf> accessed 13 November 2017, p7.
[229] ibid, p18.
[230] ibid, p26.
[231] ibid, p37.
[232] Damien Gayle, ''Downward spiral': UK slips to 40th place in press freedom rankings' *The Guardian* (London, 26 April 2017) <https://www.theguardian.com/media/2017/apr/26/uk-world-press-freedom-index-reporters-without-borders> accessed 13 November 2017; Reporters Without Borders, 'A worrying trend' (2017) <https://rsf.org/en/united-kingdom> accessed 13 November 2017.
[233] *Tillack v Belgium* App no. 20477/05 (ECHR, 27 November 2007), [65].
[234] Richard Hyde and Ashley Savage, 'Cross-border Concerns: Perils and Possibilities' (2013) E-Journal of International and Comparative LABOUR STUDIES 2:3 <http://ejcls.adapt.it/index.php/ejcls_adapt/article/viewFile/132/195> accessed 5 May 2017, 4.

The idea of freedom of expression 'regardless of frontiers' takes on a new meaning in the Internet era as it empowers individuals around the world with the potential to seek, receive, and impart information and ideas in unprecedented ways.[235] Hyde and Savage note that cross-border whistleblowing also relates to the aviation and food sector,[236] and others such as surface transportation, shipping, road haulage, energy production and financial services.[237] The ECtHR in *Ekin Associations v France*[238]ruled that restrictions on foreign publications is in direct conflict with the notion of 'regardless of frontiers' and ultimately held that Article 10 had been violated, as it was in the *Spycatcher* case.[239] It has already been noted that data retention and surveillance in general has a chilling effect on various rights protected by the ECHR, this point is more profound when considering extraterritorial surveillance. In *Human Rights Watch & Others v The Secretary of State for the Foreign & Commonwealth Office & Others*[240] the IPT ruled that Article 1 (jurisdiction) of the ECHR did not apply to the surveillance carried out by UK intelligence agency GCHQ when the individual concerned was not physically present in the UK. If Article 1 does not apply, then the corresponding rights set out in the Convention are not applicable. This position has been heavily criticised especially because the surveillance actually *did* take place within UK territory.[241] What this would mean in practice is that when communicating from abroad, whether surveillance is conducted in the territory of the UK, Convention rights do not apply. There is a risk that intelligence agencies may exploit this gap to circumvent Convention protections through the use of intelligence sharing arrangements[242] and therefore uncontrolled data retention could ensue with impunity. More worrisome is that if a person present in the UK uses a VPN and sets their location abroad, would the ECHR again be said to be not applicable? If the answer is yes, then the UK would be in violation for the simple fact that Article 1 would apply because said person *is* in the UK. This is why, whatever the location, when conducting surveillance, the ECHR should be adhered to. Failing to do so would compromise the essence of free flow of information, regardless of frontiers. Not only does this affect private life in aspects of personal development, professional activities and autonomy in general when communicating with persons abroad. It can have an impact of family life in, for example, communications between family members in different countries. This in turn relates to an interference with the correspondence aspect of Article 8, the greater propensity for a chilling effect to materialise, and thus, again, highlights the interrelation between Articles 8 and 10. The inhibitory effects of the free flow of information affects one's ability to receive and impart information.

---

[235] Center for Democracy and Technology, '"Regardless of Frontiers" The International Right to Freedom of Expression in the Digital Age' (April 2011) <https://cdt.org/files/pdfs/CDT-Regardless_of_Frontiers_v0.5.pdf> accessed 6 May 2017.

[236] Richard Hyde and Ashley Savage, (n234), p14 and p18.

[237] ibid, p4.

[238] *Ekin Associations v France* App no. 39288/98 (ECHR, 17 July 2001), [62-4].

[239] *Sunday Times v UK (No.2)* App no. 13166/87 (ECHR, 26 November 1991), [55-6].

[240] *Human Rights Watch & Others v The Secretary of State for the Foreign & Commonwealth Office & Others* [2016] IPT/15/165/CH, IPT/15/166 CH, IPT/15/167/CH, IPT/15/168/CH, IPT/15/169/CH, IPT/15/172/CH, IPT/15/173/CH, IPT/15/174/CH, IPT/15/175/CH, IPT/15/176/CH.

[241] Marko Milanovic, 'UK Investigatory Powers Tribunal Rules that Non-UK Residents Have No Right to Privacy under the ECHR' (18 May 2016) <https://www.ejiltalk.org/uk-investigatory-powers-tribunal-rules-that-non-uk-residents-have-no-right-to-privacy-under-the-echr/> accessed 6 May 2017; Scarlet Kim, 'ECHR Jurisdiction and Mass Surveillance: Scrutinising the UK Investigatory Power Tribunal's Recent Ruling' (9 June 2016) <https://www.ejiltalk.org/echr-jurisdiction-and-mass-surveillance-scrutinising-the-uk-investigatory-power-tribunals-recent-ruling/> accessed 6 May 2017.

[242] Vivian Ng and Daragh Murray, 'Extraterritorial Human Rights Obligations in the Context of State Surveillance Activities?' (2 August 2016) <https://www.hrbdt.ac.uk/extraterritorial-human-rights-obligations-in-the-context-of-state-surveillance-activities/> accessed 6 May 2017.

(g) Receive and impart information

Although not a strict form of censorship in the traditional sense used about permissions in print media, and also not a real-time delay to electronic communications, data retention may still be seen to be something that engages the strand of Article 10 ECHR encompassing the qualified right to receive and impart information.[243] Alex Matthews and Catherine Tucker demonstrated that post-Snowden revelations negatively affected (chilling effect) Google search terms deemed both personally-sensitive and government-sensitive.[244] Search data, on generic, sensitive (potentially embarrassing) and on Homeland Security's list was collected for the US and its top 40 international partners.[245] It showed that search terms deemed troubling from a personal and private perspective dropped 4%.[246] It also provides the first substantial empirical documentation of a chilling effect, both domestically and internationally, that appears to be related to increased awareness of government surveillance.[247] Moreover, the chilling effect found to be more prominent in countries that are considered US *allies* due to initial unawareness of US activities.[248] Finally, it was noted there was a decrease in health related search terms, which was argued may have an impact economic welfare of citizens.[249] This is just one example, but if individuals are deterred from making health related searches, this may affect their physical and social identity, thus hindering their autonomous development protected under private life. Jon Penney also found similar chilling effects and noted these findings have implications for the health of democratic deliberation among citizens and the health of society.[250]

As David Kaye noted, surveillance (including data collection and retention) can create a chilling effect on the freedom of expression of ordinary citizens who may self-censor for fear of being constantly tracked. This included a wide range of vulnerable groups such as racial, religious, ethnic, gender and sexual minorities, members of certain political parties, civil society, human rights defenders, professionals such as journalists, lawyers and trade unionists, victims of violence and abuse, and children. [251]

Frank La Rue highlighted the interlink between privacy and freedom of expression further noting that states cannot ensure the freedom to receive and impart information without respecting, protecting and promoting privacy. La Rue continued that[252] privacy and freedom expression are interlinked and mutually dependent where an infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequately securing privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.

---

[243] Ivana Roagna, (n12), p32.
[244] Alex Matthews and Catherine Tucker, 'Government Surveillance and Internet Search Behavior' 17 February 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564> accessed 4 May 2017.
[245] ibid, p4.
[246] ibid.
[247] ibid, p40.
[248] ibid, p33.
[249] ibid, p39.
[250] Jon Penney, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) Berkeley Technology Law Journal 31:1 117 <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2104&context=btlj> accessed 5 May 2017, 169.
[251] David Kaye, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (11 May 2016) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/12/PDF/G1609512.pdf?OpenElement> accessed 4 May 2017, para 57.
[252] Frank La Rue, (n186), para 79.

Another aspect of the freedom to receive and impart information derives from Breyer's analysis[253] that if the state does not fully compensate telecommunication operators, then prices for their services may significantly increase, or formerly 'free'[254] services may cease to be offered. Bernal and others have noted that Internet Connection Records (ICRs) are expensive and the burden of costs may also (as well as government) fall on ordinary Internet users.[255] LINX argued that costs are unlikely to be recoverable *even if* the government reimburses ISPs for the full capital costs and ongoing direct operational expenses.[256] Section 249 of the IPA 2016 deals with telecommunications operator reimbursement. Subsection(7) specifically deals with the costs of retention notices, but there is no guarantee of full remuneration because discretion is given to the Secretary of State to consider what is appropriate,[257] so long as it is not £0.[258] As Breyer notes this could have the consequence of decreasing the amount of information people can afford to circulate, which ultimately interferes with freedom of expression.[259] Being unable to (re-)circulate information may again have an indirect effect on the development of individuals protected under Article 8 and opinions under Article 10.

(h) Facts and opinion

Article 10 covers both facts and opinions.[260] The GC in noted that there is very little scope for restrictions on political speech.[261] Chapter 3 detailed how data retention interferes with political views, which is special/sensitive data, and therefore relates to data protection aspects of Article 8.

Moreover, iiNet has demonstrated that embedded data about communications like Twitter, Facebook, and websites does in fact reveal substantial amount of the content of communications (such as tweets).[262] Therefore, data retention would not just retain the communications data associated with tweets, but the actual tweets itself, making it far easier to identify individuals, thus interfering with anonymity, private life and the ability to express oneself.

This section has demonstrated the interrelation between Article 8 and Article 10 ECHR, and in many cases where the former underpins the latter. Pluralism, is established in the jurisprudence

[253] Patrick Breyer, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR' (2005) European Law Journal 11:3 365, 373.
[254] The CEO of Allstate Insurance noted that people get 'on Google, and it seems like it's free. It's not free. You're giving them information; they sell your information.' Shoshana Zuboff, 'The Secrets of Surveillance Capitalism' (5 March 2016) <http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html> accessed 22 February 2017.
[255] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, February 2016, <http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf> accessed 3 May 2017, Paul Bernal, para 8.1.1, page 139, Giuseppe Sollazzo, para 3.1.4, page 1259.
[256] ibid, LINX, para 27(d), page 915.
[257] Section 249(1) of the IPA 2016.
[258] Section 249(6) of the IPA 2016.
[259] Patrick Breyer, (n253), 373.
[260] *Lingens v Austria* App no. 9815/82 (ECHR, 8 July 1986), [46]; Patrick Breyer, (n253), 373.
[261] *Mouvement raëlien Suisse v Switzerland* App no. 16354/06 (ECHR, 13 July 2012), [61].
[262] iiNet, 'Protecting your privacy: Our stand against 'mandatory data retention'' (21 July 2014) <http://blog.iinet.net.au/protecting-your-privacy/> accessed 30 December 2016.

of the ECtHR, especially when it comes to freedom of expression and religion.[263] An interrelationship between Article 10 and 9 is argued to exist.[264] The Steering Committee of the CoE on Media and Information Society (Steering Committee) noted that the Internet allows the expression of political convictions, as well as *religious and non-religious views* which concerns the right to freedom of thought, conscience and religion as enshrined in Article 9 of the ECHR.[265]

4.7 Freedom of Religion, Thought, Conscience and Article 9 ECHR

Article 9(1) ECHR notes:

> Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief and freedom, either alone or in community with others and in public or private, to manifest his religion or belief, in worship, teaching, practice and observance.

The CoE's Parliamentary Assembly agreed that surveillance (including data retention)[266] endangers freedom of religion.[267] It's CFR equivalent is Article 10.

(a) General Principles

Freedom of religion is regarded as one of the foundations of a democratic society within the meaning of the Convention. It is, in its religious dimension, one of the most essential elements of the identity of believers and their conception of life, but it is also a precious asset for atheists, agnostics, skeptics and the unconcerned[268] and humanists.[269] That freedom entails, inter alia, freedom to hold or not to a religion and that to practice or not to practice it.[270] The aspect of 'identity of believers' relates to the social identity aspect of private life as discussed above.

(b) Freedom to Manifest a Belief

The freedom to manifest one's religion can be done in public or in private.[271] This closely relates with the private life aspect of Article 8 which can be considered in conjunction.[272] The freedom to manifest one's religion also encompasses the ability to convince one's neighbour

---

[263] Aernout Nieuwenhuis, 'The Concept of Pluralism in the Case-Law of the European Court of Human Rights' (2007) European Constitutional Law Review 3: 367.
[264] Julie Maher, 'Proportionality analysis after Eweida and Others v. UK: Examining the Connections between Articles 9 and 10 of the ECHR' (June 2013) <http://ohrh.law.ox.ac.uk/proportionality-analysis-after-eweida-and-others-v-uk-examining-the-connections-between-articles-9-and-10-of-the-echr/> accessed 6 May 2017.
[265] Steering Committee on Media and Information Society (CDMSI) (16 April 2014) <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c6f85#P118_25200> accessed 6 April 2017, para 40.
[266] Pieter Omtzigt, Committee on Legal Affairs and Human Rights, 'Mass surveillance' (26 January 2015) <http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10b7a2> accessed 8 May 2017, para 78.
[267] Resolution 2045 (2015), <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/resol_mass_surveillance_/resol_mass_surveillance_en.pdf> accessed 8 May 2017, para 4.
[268] *Buscarini and Others v San Marino* App no. 24645/94 (ECHR, 18 February 1999), [34].
[269] *Smyth, Re Judicial Review* [2017] NIQB 55, [48].
[270] *Buscarini and Others*, (n268), [34].
[271] *Ivanova v Bulgaria* App no. 52435/99 (ECHR, 12 April 2007), [78].
[272] *S.A.S v France* App no. 43835/11 (ECHR, 1 July 2014), [107-110].

i.e. through teaching.[273] Although there is a differentiation the ECtHR in *Campbell and Cosans v the United Kingdom*[274] differentiated between opinions/ideas and belief, [275] it still relates to the freedom to impart *information* aspect of Article 10 and can be considered in conjunction with Article 9 if it is necessary[276] or relates to religion.[277] This would ultimately also relate to the freedom to *receive* information under Article 10 and respecting correspondence under Article 8, and therefore, ultimately freedom of communication.

(c) Freedom to Hold a Belief

The right to hold a belief is unconditional and absolute.[278] This relates to the personal autonomy aspect of private life in that 'autonomy is salient in the reasoning of the Court and most notably under Article 9.'[279]

(d) Article 9 and its relationship with Data Retention

In *Sinan Isik v Turkey* the ECtHR noted that:

> [T]he right to manifest one's religion or beliefs also has a *negative aspect, namely an individual's right not to be obliged to disclose his or her religion or beliefs and not to be obliged to act in such a way that it is possible to conclude that he or she holds – or does not hold – such beliefs.* Consequently, *State authorities are not entitled to intervene in the sphere of an individual's freedom of conscience and to seek to discover his or her religious beliefs or oblige him or her to disclose such beliefs*.[280]

It has already been noted Chapter 3 how communications data can reveal philosophical or religious beliefs.[281] Data retention forces the disclosure of religion or belief via State intervention through retention notices which for example, captures web history. Therefore, the mere existence of data retention laws likely interferes with Article 9 because it makes it possible to conclude whether one holds a religion or belief. This also establishes another link with Article 8 as the mere storage of personal data interferes with private and family life.[282] This interferes with the data protection aspect of Article 8 more profoundly because religion is classed as sensitive/special data and thus the rules on processing become stricter. Due to the state 'intervening' by retaining this data, another aspect of private life arises, that is of personal development which can be inhibited by the reluctance to seek out information due to the chilling effect discussed throughout this Chapter. This therefore again becomes an Article 8 *and* Article 10 issue. Another aspect of the interrelation between Article 9 and Article 8 is the correspondence aspect, although concerning interception (which is actually possible through

[273] *Ivanova*, (n271), [78].
[274] *Campbell and Cosans v the United Kingdom* App no 3578/05 (ECHR, 25 February 1982), [36]
[275] ibid.
[276] *Glas Nadezhda Eood and Anatoliy Elenkov v Bulgaria* App no. 14134/02 (ECHR, 11 October 2007), [59].
[277] *Murphy v Ireland* App no. 44179/98 (ECHR, 10 July 2003), [60-1].
[278] *Ivanova*, (n271), [79].
[279] Begum Bulak and Alain Zysset, '"Personal Autonomy" and "Democratic Society" at the European Court of Human Rights: Friends or Foes?' (2013) UCL Journal of Law and Jurisprudence 2 <http://discovery.ucl.ac.uk/1470685/1/2UCLJLJ230%20-%20Personal%20Autonomy.pdf> accessed 8 May 2017, p248.
[280] *Sinan Isik v Turkey* App no. 21924/05 (ECHR, 2 February 2010), [41].
[281] Paul Bernal, (n4), 253.
[282] *Folberø and Others v Norway* App no. 15472/02 (ECHR, 29 June 2007), [98].

Part 4),[283] data retention also threatens the privileged communications of religious ministers,[284] thus striking at the freedom of communication, which in turn can have an effect on their professional activities, also protected under private life. It has also been shown that surveillance can have a chilling effect on those practising a particular religion. It was statistically confirmed that 'that Muslim-Americans not only believe the government monitors their routine activities, but that such concerns have translated into actual changes in daily behavior.'[285]

In regards to conscience, Bernal notes that Apple, Google and Microsoft's 'digital assistants,' Siri, Now and Cortana all aim to predict what one knows, to the extent that Google and Facebook can know people better than they know themselves.[286] One reason is due to self-deception,[287] the other is the frailty of human memory, something that Google is not prone to because it remembers perfectly, *forever* (author's emphasis).[288] This may raise issues (already touched upon by the CJEU)[289] of the right to be forgotten and data portability where 'the right for the data subject to object to the further processing of his/her personal data, and an obligation for the data controller to delete information as soon as it is no longer needed for processing.'[290] The right to be forgotten, or as Bernal phrases it, a right to delete[291] is currently being considered by the ECtHR in *M.L. v. Germany and W.W. v. Germany* under Article 8.[292]

Moving on from predictability, Facebook has announced that it seeks to develop technology that would be able *to read a person's mind* in order to communicate.[293] Neuroscientist Mark Chevillet hinted that Facebook's goal would require non-invasive sensors to detect brain signals associated with word thinking, algorithms to figure out the intended word, Artificial Intelligence (AI) to aid the algorithm and technology called 'diffuse optimal tomography' which would shine infra-red light onto brain tissue to deduce patterns of neurons based on light scattered.[294] Such neurotechnologies have applications in device control, real-time neuromonitoring, neurosensor-based vehicle operator systems, cognitive training tools, electrical and magnetic brain stimulation, wearables for mental wellbeing, virtual reality systems and for everyday activities including gaming, entertainment, and smart- phone's remote control.[295] Apple and Samsung are incorporating neurogadgets into their major

[283] See Chapter 3.
[284] Pieter Omtzigt, (n266), para 4.
[285] Dawinder S. Sidhu, 'The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim Americans' (2007) 7 U. Md. L.J. Race Relig. Gender & Class 375 7:2: <http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1134&context=rrgc> accessed 12 May 2017.
[286] Paul Bernal, (n4), 253-4.
[287] ibid, 254.
[288] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W.W. Norton 2016), 26.
[289] Case C-131/12, *Google Spain SL v Agencia Española de Protección de Datos, González* [2014] E.C.R. 317.
[290] Council of Europe Research Division, 'Internet: case-law of the European Court of Human Rights' (June 2015) <http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf> accessed 8 May 2017, p14.
[291] Paul Bernal, (n185), 200-206.
[292] *M.L. v Germany and W.W. v Germany* App nos. 60798/10 and 65599/10, communicated to the respondent Government under Article 8 of the Convention on 29 November 2012.
[293] Olivia Solon, 'Facebook has 60 people working on how to read your mind' *The Guardian* (London, 19 April 2017) <https://www.theguardian.com/technology/2017/apr/19/facebook-mind-reading-technology-f8> accessed 24 April 2017.
[294] Kristen V. Brown, 'Here Are the First Hints of How Facebook Plans to Read Your Thoughts' *Gizmodo* (21 September 2017) <https://gizmodo.com/here-are-the-first-hints-of-how-facebook-plans-to-read-1818624773> accessed 9 November 2017.
[295] Marcello Ienca and Roberto Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology' (2017) Life Sciences, Society and Policy 13:5 1, 4

products.[296] It was predicted that neurodevices would gradually replace the keyboard, mouse, touchscreen and voice command as the preferred way to interact with computers.[297] This will lead to an increase the availability of brain information to third parties, exposing them 'to the same degree of intrusiveness and vulnerability to which is exposed any other bit of information circulating in the digital ecosystem.'[298]

The mind is a 'kind of last refuge of personal freedom and self-determination.'[299] The risks of using brainwaves to eavesdrop and gain passwords[300] is already here, which is matched by calls for human rights to protect mental privacy, cognitive liberty, mental integrity and psychological continuity.[301] Cognitive liberty is synonymous with freedom of thought[302] yet more precisely evokes the idea 'individuals should have the right to autonomous self-determination over their own brain chemistry.'[303] It is necessary for all other liberties.[304] For Bublitz, an aspect of cognitive liberty entails the protection of individuals of coercive or unconsented use of neurotechnologies.[305] This may have implications for Article 9, if data from neurotechnologies are to be retained because this would fall under 'unconsented use.' Moreover, unlike Articles 8, 10 and 11, the restrictions of Article 9 apply only to the *manifestation* of religion and beliefs, not the thoughts themselves,[306] as they are absolute (author's emphasis).[307]If neurotechnologies can be used to discern the contents of thoughts against one's will (non-consent)[308]'it would have a chilling effect not only on expression but also on the source of expression, and thus it would impact the freedom people have even to entertain those thoughts.'[309] The very notion of freedom of thought could very well be put

[296] ibid.
[297] ibid.
[298] ibid, 12.
[299] ibid, 1.
[300] Ajaya Neupane, Lutfor Rahman and Nitesh Saxena, 'PEEP: Passively Eavesdropping Private Input via Brainwave Signals' (2017) <https://info.cs.uab.edu/saxena/docs/nrs-fc17.pdf> accessed 5 September 2017; Charlie Osborne, 'How hackers can hijack brainwaves to capture your passwords' (8 May 2017) <http://www.zdnet.com/google-amp/article/how-hackers-use-brainwaves-to-capture-your-passwords/?utm_content=buffer5b8d1&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer > accessed 5 September 2017; Tom Simonite, 'Using Brainwaves to Guess Passwords' (5 May 2017) <https://www.technologyreview.com/s/604293/using-brainwaves-to-guess-passwords/?set=604330> accessed 5 September 2017.
[301] Marcello Ienca and Roberto Andorno, (n295); Marcello Ienca, 'Do We Have a Right to Mental Privacy and Cognitive Liberty?' (3 May 2017) <https://blogs.scientificamerican.com/observations/do-we-have-a-right-to-mental-privacy-and-cognitive-liberty/> accessed 11 October 2017; Sarah Richmond, Geraint Rees and Sarah J. L. Edwards, *I Know What You're Thinking: Brain imaging and mental privacy* (Oxford University Press 2012); Jesper Ryberg, 'Neuroscience, Mind Reading and Mental Privacy' (2017) Res Publica 23:2 197; Francis X. Shen, 'Neuroscience, Mental Privacy, and the Law' (2013) Harvard Journal of Law & Public Policy 36:2 653; Woodrow Barfield and Alexander Williams, 'Law, Cyborgs, and Technologically Enhanced Brains' (2017) Philosophies 2:6.
[302] Marcello Ienca and Roberto Andorno, (n295), 10.
[303] Charlotte Walsh, 'Psychedelics and Cognitive Liberty: reimagining drug policy through the prism of human rights' (2016) International Journal of Drug Policy 29: 80, 83.
[304] Marcello Ienca and Roberto Andorno, (n295), 10.
[305] Jan-Christoph Bublitz, 'My Mind Is Mine!? Cognitive Liberty as a Legal Concept' in Elisabeth Hildt and Andreas G. Franke (ed), *Cognitive Enhancement An Interdisciplinary Perspective* (Dordrecht: Springer 2013), 234.
[306] *Ivanova*, (n271), [79].
[307] Charlotte Walsh, (n303), 83; Marcello Ienca and Roberto Andorno, (n295), 15.
[308] Stephen Mumford and Rani Lill Anjum, 'Powers, Non-Consent and Freedom' (2014) Philosophy and Phenomenological Research 91:1 136.
[309] Adina L. Roskies, 'Mind Reading, Lie Detection, and Privacy' in Jens Clausen and Neil Levy (ed), *Handbook of Neuroethics* (Springer Netherlands 2015), 687.

under threat as retention of thought data could be seen as taking 'coercive steps to make him change his beliefs.'[310]

Several questions arise, under what conditions could brain information be collected, what components shall be disclosed and made accessible to others, who should access this and what should be the limits to consent in the area?[311] It was noted that neurotechnologies creates risk of unparalleled intrusion into the private sphere causing physical or psychological harm or unduly influencing one's behaviour.[312] For Ienca and Andorno, the mere collection of brain data can violate mental privacy.[313] Brain signals also allow the tracing or distinguishing of one's identity.[314] This establishes a link between Article 9 and 8 in that this would touch upon aspects of the latter with regards to physical, psychological and moral integrity, identity, autonomy, informational self-determination and data protection. However, Ienca and Andorno argue that privacy and data protection are insufficient to deal with emerging neurotechnological scenarios, hence the need for the formal recognition of mental privacy.[315] For example, Article 8 is a relative, rather than an absolute right, as some argue probing the mind against one's will should be prohibited in all circumstances.[316] This raises no issues, if this falls within the ambit of freedom of thought in Article 9, but with Article 8, it may well be justifiable. Falling under the later, it would be argued that the State's margin of appreciation should be even narrower than retention of other forms of communications data as this would be of the utmost sensitivity. An alternative would be for the CoE to adopt an Additional Protocol dealing specifically with mental privacy. However, for these purposes, it is argued that Article 9 would be the best protection currently available due to its absolute nature of freedom of thought and conscience.

Given that smart phones, devices and apps are covered by the IPA 2016,[317] retention of thought data would truly encompass what Caspar Bowden highlighted when he coined the term 'CCTV (or Big Brother)[318] for inside your head.'[319] Thus, ultimately interfering with one's conscience. The GC has noted where 'the organisation of the religious community is at issue, Article 9 of the Convention must be interpreted in the light of Article 11.'[320] For this reason, it is necessary to now consider data retention and its implications on Article 11.

4.8 Article 11 ECHR

Article 11(1) maintains that:

> Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.

---

[310] *Ivanova*, (n271), [79].
[311] Marcello Ienca and Roberto Andorno, (n295), 12.
[312] ibid, 2.
[313] ibid, 15.
[314] ibid, 14.
[315] ibid, 15.
[316] ibid, 15-16.
[317] See Chapter 6.
[318] Celia Gorman, 'The Mind-Reading Machine' (9 July 2012) <https://spectrum.ieee.org/biomedical/diagnostics/the-mindreading-machine> accessed 9 November 2017.
[319] Caspar Bowden, 'CCTV for inside your head Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation' (2001) <http://europe.rights.apc.org/eu/cctv_for_the_head.html> accessed 24 April 2017.
[320] *Hasan and Chaush v Bulgaria* App no. 30985/96 (ECHR, 26 October 2000), [62].

Article 12 CFR is Article 11's equivalent.

(a) The Importance of Freedom of Association

Zvonimir Mataga argues that freedom of association enables individuals to protect their rights and interests in alliance with others.[321] Mataga continues that such possibility is of the utmost importance since, from a sociological aspect, association means creation or accession to an organisation – which is due to its characteristics able to achieve goals which an individual alone would not be able to achieve at all, or at least not effectively. This also relates to the very important aspect of private life in that it protects individual's right to develop and form relationships with the outside world. Manfred Nowak highlighted the dualist nature of freedom of association as granting civil and political rights. Regarding the civil rights aspect, freedom of association protects against arbitrary interference by the State or private parties when, for whatever reason and for whatever purpose, an individual wishes to associate with others or has already done so. From the political rights perspective, it is indispensable for the existence and functioning of democracy, because political interests can be effectively championed only in community with others (as a political party, professional interest group, organization or other association for pursuing particular public interests).[322] The civic and political freedoms aspect was also noted by the GC in *Zdanoka v Latvia*.[323] Moreover, the GC has also 'on numerous occasions affirmed the direct relationship between democracy, pluralism and the freedom of association.'[324]

(b) The Importance of Freedom of Assembly

The GC too has stressed the importance of freedom of assembly where they noted that 'the right to freedom of assembly is a fundamental right in a democratic society and, like the right to freedom of expression, is one of the foundations of such a society.'[325] Moreover it was noted that measures to supress freedom of assembly other than in cases of incitement to violence or rejection of democratic principles – however shocking and unacceptable words used and however illegitimate demands made may be, may endanger democracy.[326]

(c) Differentiating Assembly from Association and their respective application

In order to highlight the significance of freedom of assembly and association in respect of data retention, it is first necessary to distinguish between both concepts. The idea of freedom of association encompasses the right to form or be affiliated with a group or organisation pursuing particular aims.[327] Article 11 affords protection to any group considered an association.[328]According to Mataga, associations within the meaning of Article 11 has an

[321] Zvonimir Mataga, 'The Right to Freedom of Association Under the European Convention on the Protection of Human Rights and Fundamental Freedoms' (October 2006) <http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan044376.pdf> accessed 9 May 2017, p4.
[322] Manfred Nowak, *UN Covenant on Civil and Political Rights. CCPR Commentary* (2nd rev. ed.). (Kehl am Rhein: Engel, 2005), 385.
[323] *Zdanoka v Latvia* App no. 58278/00 (ECHR, 16 March 2006), [115].
[324] *Gorzelik and Others v Poland* App no. 44158/98 (ECHR, 17 February 2004), [88].
[325] *Kudrevićius and Others v Lithuania* App no. 37553/05 (ECHR, 15 October 2015), [91].
[326] *Güneri and Others v Turkey* App no. 42853/98 (ECHR, 12 July 2005), [76].
[327] *McFeeley v UK* App no. 8317/78 (ECHR, 15 May 1980), [114].
[328] *United Communist Part of Turkey and Others v Turkey* App no. 19392/92 (ECHR, 30 January 1998), [33-4].

autonomous meaning independent of state classifications.[329] For the ECtHR, 'association' presupposes 'a voluntary grouping for a common goal.'[330] Although trade unions are specifically mentioned in Article 11, the ECtHR interprets the term 'association' very broadly to include a number of form of associations. This includes the right to join and form associations, (especially) political parties, religious organisations, employer associations, companies and various other forms of association,[331] including environmental associations.[332] Moreover, Article 11 protects informal associations provided that they fulfil the minimum degree of organisation and size and companies.[333]

What distinguishes association from assembly is the:

(i) higher degree of institutional organisation (does not require legal status, requires more than mere social gathering, and some degree of continuity);
(ii) voluntary character; and
(iii) the pursuit of a common goal (for mutual or public benefit).[334]

The GC regards that assembly should not be interpreted restrictively, as the right covers both private meetings and meetings in public places, whether static or in the form of a procession; in addition, it can be exercised by individual participants and by the persons organising the gathering.[335]

(d) Association and Assembly in the Digital Age

In their paper, Douglas Rutzen and Jacob Zenn argue that freedom of association and assembly applies to online communities i.e. Facebook groups, social networks.[336] Although using slightly different criteria[337] for determining what constitutes association, it will be argued this is still applicable to the ECtHR's interpretation. Rutzen and Zenn use the examples of '"April 6 Movement" that originated in Egypt; the "One Million Voices Against FARC" that originated in Colombia; and "Mir Hussein Mousavi's" Facebook page that originated in Iran.'[338]

Movement	Description
April 6 Movement	Facebook group, reported on strikes, alerted online networks about police activity, organised protests against illegal government activity, obtained over 100,000 members by 11 March 2011, and promoted 'millions march.'

[329] Zvonimir Mataga, (n321), p5.
[330] *Young, James and Webster v UK* App nos. 7601/76 and 7896/77 (ECHR, 14 December 1979), [167]; Manfred Nowak, (n322), 496.
[331] Zvonimir Mataga, (n321), p5.
[332] *Costel Popa v Romania* App no. 47558/10 (ECHR, 26 April 2016).
[333] Zvonimir Mataga, (n321), p5-6.
[334] Dragan Golubovic, 'Freedom of association in the case law of the European Court of Human Rights' (2013) The International Journal of Human Rights, 17:7-8 758, 761-3.
[335] *Kudrevićius and Others*, (n325), [91].
[336] Douglas Rutzen and Jacob Zenn, 'Association and Assembly in the Digital Age' (2011) The International Journal of Not-for-Profit Law 13:4.
[337] ibid.
[338] ibid.

One Million Voices Against FARC	Facebook group, based on concern about FARC's actions, acquired 100,000 members within a week, highly organised – setting up officer roles on issues of legal reform to public relations, coordinated community organisers spanning nearly 50 countries to raise funds for advertising campaign and to plan protest that reached between 500,000 and 2 million.
Mir Hussein Mousavi's	Facebook page, providing a framework for citizen journalism, sought to raise awareness of events happening in Iran to gain inside and outside support.[339]

Rutzen and Zenn detailed that each group had what the ECtHR would consider a common goal. As they were Facebook groups, membership was voluntary (though individuals can be added to Facebook groups by others, they can also remove themselves). Finally, as Rutzen and Zenn note, the original creators 'provided leadership and institutional structure to their organisations.'[340] These would qualify as 'associations' not only under international law[341] but also under the Article 11 ECHR.

Regarding assembly, Rutzen and Zenn noted this is also covered online referring to online government petitions as an example.[342] As noted above, the ECtHR has noted that assembly includes public and private meetings *whether static* or in the form of demonstrations. Therefore, physical proximity is not necessary as private static meetings could include Skype meetings,[343] Whatsapp Group Chat,[344] and public static meetings could include livestreaming conferences via Youtube.[345]

To further add to this, it serves as a reminder that the UN and CoE have already maintained that rights available offline should be readily available online also. The Steering Committee in their guide (as recommended by the Committee of Ministers (CoM)[346] to human rights for Internet users when referring to Article 11 noted that users have 'the right to peacefully assemble and associate with others using the Internet.'[347] They continued that this included 'forming, joining, mobilising and participating in societal groups and assemblies as well as in trade unions *using Internet-based tools* (author's emphasis).'[348] This includes signing of petitions (as Rutzen and Zenn mention above) to participate in a campaign or other forms of

[339] ibid.
[340] ibid.
[341] ibid.
[342] ibid.
[343] Skype for Business Team, 'Introducing free Skype Meetings' (5 July 2016) <https://blogs.office.com/2016/07/05/introducing-free-skype-meetings/> accessed 10 May 2017.
[344] Whatsapp, 'How do I use Group Chat?' <https://www.whatsapp.com/faq/en/iphone/23782517> accessed 10 May 2017.
[345] Pexip, 'Streaming a conference over YouTube' <https://docs.pexip.com/admin/streaming_youtube.htm> accessed 10 May 2017.
[346] Recommendation CM/Rec(2014)6 and explanatory memorandum.
[347] Steering Committee on Media and Information Society (CDMSI), (n268), para 61.
[348] ibid.

civic action.[349] Crucially, the Steering Committee noted that 'user should have the *freedom to choose the tools* for the exercise of the rights such as *websites, applications or other services* (author's emphasis).'[350] This would, therefore, put in a whole ranges of services beyond those (Skype, Whatsapp and Youtube) mentioned above. Formal recognition of social groups, in line with Article 11 is not required, moreover, online protests are permissible subject to limitations.[351] This overwhelmingly demonstrates how online association and assembly are protected under Article 11. What binds the online aspect of freedom of assembly and association, is the freedom of communication with others. Albeit briefly discussed above, Mataga noted that Article 11 has relationships with other Convention Rights.[352]

(e) *Interrelation between Article 11 and 8-10*

The relationship between Article 10 and 11 has been highlighted by the GC in *United Communist Party of Turkey and others v Turkey* that:

> [N]otwithstanding its autonomous role and particular sphere of application, Article 11 must also be considered in the light of Article 10. The protection of opinions and the freedom to express them is one of the objectives of the freedoms of assembly and association as enshrined in Article 11… That applies all the more in relation to political parties.[353]

Regarding the relationship with Article 9, the ECtHR has ruled Article 11 needs to be interpreted in light of Article 9 as it includes the freedom, either alone or in community with others and in public or private, to manifest one's religion or belief, in worship, teaching, practice and observance.[354] Furthermore, in *Young, James and Webster v United Kingdom* the ECtHR ruled that '[t]he protection of personal opinion afforded by Articles 9 and 10…in the shape of freedom of thought, conscience and religion and of freedom of expression is also one of the purposes of freedom of association as guaranteed by Article 11 (art. 11).'[355] Articles 9-11 'are designed to protect the freedom to share and express opinions, and to try to persuade others to one's point of view, *which are essential political freedoms in any democracy*.'[356]

The GC recognises that freedom of association is particularly important for persons belonging to minorities, including national and ethnic minorities, and that, as laid down in the preamble to the Council of Europe Framework Convention:

> [A] pluralist and genuinely democratic society should not only respect the ethnic, cultural, linguistic and religious identity of each person belonging to a national minority, but also create appropriate conditions enabling them to express, preserve and develop this identity. [357]

[349] ibid.
[350] ibid.
[351] ibid, para 61-2.
[352] Zvonimir Mataga, (n321), p28.
[353] *United Communist Part of Turkey and Others*, (n224), [42-3].
[354] Zvonimir Mataga, (n321), p28.
[355] *Young, James and Webster*, (n330), [57].
[356] *Countryside Alliance and others*, (n161), [118].
[357] *Gorzelik and Others*, (n324), [93].

Moreover, it was noted that 'forming an association in order to express and promote its identity may be instrumental in helping a minority to preserve and uphold its rights.'[358] This establishes a link between association and ethnic identity (mentioned above) in which a lack of respect is capable of impacting on the group's sense of identity and the feelings of self-worth and self-confidence of members of the group. This can be seen as affecting the private life of members of the *group*.[359]

Both Golubovic[360] and Mataga[361] have noted the relationship between Article 11 and the aspect of 'home' in Article 8 when referring to *Niemetz v Germany*, due to it including business premises.[362] Due to Article 8 being applicable to natural and legal persons,[363] Mataga argues that 'it would follow that business premises of an association also fall to be protected under Article 8 of the Convention.'[364]

Regarding assembly, Valerie Aston notes that there is a 'significant overlap between interference in privacy rights and those relating to the restriction of assembly.'[365] In *Sørensen and Rasmussen v Denmark* the GC noted that personal autonomy 'must therefore be seen as an essential corollary of the individual's freedom of choice implicit in Article 11 and confirmation of the importance of the negative aspect of that provision.'[366] Autonomy non-exhaustively interlinks Articles 8-11 in more ways than one (see above). The interlinks become more apparent when considering association, assembly and data retention.

(f) Data Retention and Freedom of Association and Assembly

As Mataga has noted, '[a]n interference with the freedom of association will normally not be caused by the law itself…even though such a situation would also be conceivable, but rather by a decision…given in applying that law.'[367] Interference could be established in both cases. First, following the *Klass* approach, that the mere existence of surveillance laws which can be applied to anyone interferes with Article 11. This is because retention of data that relates to association or assembly necessarily interferes with Article 11. As Bernal notes, the knowledge of the existence of surveillance can produce more conformist behaviour which would impact directly on the willingness to exercise the freedom of both assembly and association.[368] Bernal further notes that this will increase due to the increasing interactions between technologies, geolocation and the Internet of Things (IoT).[369] For Bernal, the power effect of gathering data and holding it impacts upon autonomy.[370] Secondly, this is supported by the approach in *Segerstedt-Wiberg and Others v Sweden*, the ECtHR has acknowledged that the *storage* of personal data related to *affiliations and activities* engages Article 11.[371] Using the *Klass* and

[358] ibid.
[359] *Aksu*, (n54), [58].
[360] Dragan Golubovic, (n334), 763.
[361] Zvonimir Mataga, (n321), p29.
[362] *Niemetz v Germany*, (n75), [29-33].
[363] *Société Colas Est and others v France* App no. 37971/97 (ECHR, 16 April 2002), [40-42].
[364] Zvonimir Mataga, (n321), p29.
[365] Valerie Aston, (n61), p4.
[366] *Sørensen and Rasmussen v Denmark* App nos. 52562/99 and 52620/99 (ECHR, 11 January 2006), [54].
[367] Zvonimir Mataga, (n321), p16.
[368] Paul Bernal, (n4), 256.
[369] ibid, 257.
[370] Ibid.
[371] *Segerstedt-Wiberg and Others*, (n202), [107].

Segerstedt approach, the mere existence of data retention laws and actual retention of association/assembly data therefore interferes with Article 11 and requires justification. This, of course, also relates to the data protection aspect of private and family life.

So, the question becomes, what communications data could be classed as association/assembly data? There are a multitude of data, (given that association and assembly also applies online) for example, an email address or a phone number of a known association. This could also include web history which reveals a list of e.g. environmental association websites visited. The communications data from social media accounts that are used to spread protest messages and to boycott products is an example of communications data pertaining to online assembly. The time, duration, location of a Skype chat of a e.g. Greenpeace meeting. This leads on to a very specific type of communications data, location data.[372] Bruce Schneier pointed out that 'location information is valuable, and everyone wants access to it.'[373] Rozemarijn van der Hilst argued that location data could be considered 'sensitive personal data'[374] or 'special category of personal data.'[375] This is due to the fact that '[a]ggregated location data can reveal information about a person's habits, *(future) whereabouts* (author's emphasis).'[376] This highlights not only that location data can reveal very intimate details, it can be used to make future predictions based on current data possessed.[377] It can also reveal someone's religion,[378] which would as noted above, engage Article 8, due to it being sensitive personal data, and Article 9 due to the storage of data which can make said religion identifiable. All in all, communications data (especially entity data) retention can reveal an entire life.[379] Therefore the data can reveal, who is associated with who, who organised what, who demonstrate where and when.

Another way to establish interference is by restriction. Mataga notes that '[m]easures restricting the right to freedom of association will usually fulfil' the condition of interference.[380] Regarding assembly, the ECtHR has noted that 'interference with the right to freedom of assembly does not need to amount to an outright ban, legal or de facto, *but can consist in various other measures taken by the authorities* (author's emphasis).'[381] Restrictions can include both 'measures taken before or during a gathering and those, such as punitive measures, taken afterwards.'[382] It was noted that a ban could have a chilling effect on

[372] See Chapter 4.
[373] Bruce Schneier, (n289), 2.
[374] Rozemarijn van der Hilst, 'Characteristics and uses of selected detection technologies, including their potential human rights' (30 November 2011) <http://www.detecter.bham.ac.uk/pdfs/17_3_tracking_technologies.doc> accessed 13 April 2017, p33.
[375] ibid, p38.
[376] ibid.
[377] Daniel Ashbrook and Thad Starner, 'Using GPS to learn significant locations and predict movement across multiple users' (2003) Pers. Ubiquitous Comput 7:5 275; Marta C. Gonza´lez, Ce´sar A. Hidalgo and Albert-La´szlo´ Baraba´si, 'Understanding individual human mobility patterns' (2008) Nature 453 779; Lars Backstrom, Eric Sun and Cameron Marlow, 'Find Me If You Can: Improving Geographical Prediction with Social and Spatial Proximity' (2008) <http://cameronmarlow.com/media/backstrom-geographical-prediction_0.pdf> accessed 14 April 2017.
[378] Mark N. Gasson, Eleni Kosta, Denis Royer, Martin Meints, and Kevin Warwick, 'Normality Mining: Privacy Implications of Behavioral Profiles Drawn from GPS Enabled Mobile Phones' (2011) IEEE Transactions on Systems, Man and Cybernetics 41:2 251, 258.
[379] Kai Biermann, 'Betrayed by our own data' (10 March 2011) <http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz> accessed 13 April 2017.
[380] Zvonimir Mataga, (n321), p16.
[381] *Ibrahimov and Others v Azerbaijan* App nos. 69234/11 69252/11 69335/11 (ECHR, 11 February 2016), [70].
[382] ibid.

participation and thus create interference.[383] However, from a data retention perspective, a ban is not the important ingredient, it is the fact that the ECtHR acknowledges that a *chilling effect* can give rise to interferences with Article 11. van der Hilst has noted that the 'blanket and indiscriminate retention of sensitive personal data over a longer period of time can have a *severe 'chilling effect'* (author's emphasis).' He continued that this may 'reduce people's willingness to participate in public life, which is a loss for the democratic functioning of society.'[384] Jillian York has highlighted the link between harmful effects of surveillance on freedom of expression and association in that 'metadata…and its *wide-scale capture creates a chilling effect on speech and association* (author's emphasis).'[385] There has been evidence[386] from a US perspective of surveillance causing chilling effects. The Electronic Frontier Foundation (EFF), in a case against the NSA have also argued that the collection of phone records violates the US First Amendment as it discourages 'members and constituents from associating and communicating with them for fear of being spied on.'[387] Aston notes that the [t]he fear that information may be transferred as a result of surveillance activities is itself restrictive of autonomy, *whether or not information is retained or disseminated in any particular case* (author's emphasis).'[388]

In *Gillan and Quinton* the applicants argued that a laws existence could have an intimidatory and chilling effect on the exercise of those rights. The ECtHR left open the question of whether the mere existence of stop and search powers interfered with Article 10 and 11.[389] Although the question concerned stop and search powers, the problem of chilling effects has been well documented throughout this Chapter, and therefore relevant in this context. The definition of serious crime for data retention purposes are undergoing amendments to comply with *Tele2 and Watson*.[390] Serious crime does have a definition in the IPA 2016 through s.263(1) in three parts. The third is pertinent to this discussion here in which serious crime is defined as conduct by a large number of persons in pursuit of a common purpose. First, it must be noted that person is defined in s.81 of the Regulation of Investigatory Powers Act 2000 (RIPA 2000) (and not in the IPA 2016) as including (therefore not limited to) 'any organisation and *any association* or combination of persons.' Therefore, it is made explicit by virtue of RIPA 2000, that being part of association in pursuit of a common purpose (which by definition is one of the ingredients of an association) could be regarded as serious criminals. The definition of serious crime equally applies to assembly. This is problematic because 'common purpose' is not defined.[391] Any

[383] ibid.
[384] Rozemarijn van der Hilst, 'Ranking, in terms of their human rights risks, the detection technologies and uses surveyed in WP09' (2011) <http://www.detecter.bham.ac.uk/pdfs/17_4_human_rights_ranking_of_technologies.doc> accessed 12 May 2017.
[385] Jillian York, 'The harms of surveillance to privacy, expression and association' (2014) <https://giswatch.org/en/communications-surveillance/harms-surveillance-privacy-expression-and-association> accessed 12 May 2017.
[386] Elizabeth Stoycheff, 'Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring' (2016) Journalism & Mass Communication Quarterly 93:2 296.
[387] Karen Gullo, 'Surveillance Chills Speech—As New Studies Show—And Free Association Suffers' (19 May 2016) <https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-free-association> accessed 12 May 2017.
[388] Valerie Aston, (n61), p4.
[389] *Gillan and Quinton v UK* App no. 4158/05 (ECHR, 12 January 2010), [88-90].
[390] Home Office, 'Open consultation Investigatory Powers Act 2016' (30 November 2017) <https://www.gov.uk/government/consultations/investigatory-powers-act-2016> accessed 15 January 2018.
[391] Matthew White, 'Protection by Judicial Oversight, or an Oversight in Protection?' (2017) Journal of Information Rights, Policy and Practice 2:1 1, 26; See *Singh, R (on the application of) v Chief Constable of West Midlands Police* [2006] EWCA Civ 1118 in which Lady Justice Hallett gives the leading judgement noting that s.30 of Anti-social Behaviour Act 2003 applies to protestors, [79].

meeting, any group chat, whether offline or online could, therefore, be caught if serious crime was added to the justifications of retention, and it is therefore, important to highlight that this mere possibility interferes with Article 11 *irrespective* of any chilling effect. Furthermore, if a group of persons with a common purpose satisfies the definition of *serious crime*, then it would not be unreasonable to conclude that this equally applies to regular crime (for which a retention notice currently can be issued) which can classify groups as two or more people.[392]

Just as the CJEU noted in regards to freedom of expression, the retention of communications data would have an effect on the use of means of electronic communication and thus on the exercise of freedom of association and assembly. This would therefore, strike at the freedom of communication with others, whether this is to organise associations and assemblies offline or online. Online because the necessary communications data which can highlight associations or assemblies can be revealed, and offline because location data can reveal where an individual has been, disclosing sensitive/special personal data. It is for this reason, necessary to consider the possible implications for movement in physical space, which is protected under Article 2 of Protocol 4.

4.9 Article 2 of Protocol 4 ECHR

Article 2(1) of Protocol 4 states that everyone lawfully within state territory shall have 'have the right to liberty of movement.' Article 2(3) Protocol 4 sets out that any restriction on this right, amongst other things must be in accordance with the law. The first instance of considering data retention on the possible implications on freedom of movement came from the Romanian Constitutional Court (RCC).[393] The RCC acknowledged that data retention may affect 'the exercise of the right to free movement.'[394] The RCC continued that this was due to what was being required to be retained.[395] When the RCC ruled national implementation of the DRD to be unconstitutional, one of the reasons behind this was due to the fact that Article 25 of the Constitution (Freedom of Movement) had been breached as data retention would affect the *exercise* of said right. Similar arguments were raised by Digital Rights Ireland before High Court of Ireland (HCI)[396] but was rejected because Digital Rights Ireland did not have standing as a company.[397] The argument was that the:

> [T]racking and storing of the movements of any person carrying a mobile telephone amounts to an interference with the…right to travel …insofar as it establishes a system of state-mandated surveillance of the movements of the overwhelming majority of the population.[398]

Although Digital Rights Ireland's point was rejected, the HCI left it open the issue open to natural persons as it was acknowledged that there was a 'greater force in the argument that

---

[392] Corinna Ferguson, 'Do the police have the power to break up groups of innocent friends?' *The Guardian* (London, 19 March 2010) <https://www.theguardian.com/commentisfree/libertycentral/2010/mar/19/police-power-disperse-small-groups> accessed 11 November 2017. See s.30(1)(a) of the Anti-social Behaviour Act 2003.
[393] Romania Constitutional Court, (n19).
[394] ibid.
[395] ibid.
[396] *Digital Rights Ireland Ltd -v- Minister for Communication & Ors* [2010] IEHC 221, [73]; TJ McIntyre, 'Data Retention in Ireland: Privacy, Policy and Proportionality' (2008) Computer Law & Security Review 24:4 326.
[397] *Digital Rights Ireland Ltd*, (n396), [74].
[398] TJ McIntyre, (n396).

there is a right to confidential travel within the State' but could be circumscribed in the interests of preventing crime.[399] Movements and activities, offline and on are now leaving a 'footprint' in the form of traffic data which synthesize the puzzle of our everyday movements.[400] Data retention symbolises the 'disappearance of disappearance' putting freedom of movement in jeopardy,[401] because it ties in with autonomy.[402] As Mitrou points out, this is anchored in Article 2 Protocol 4 because it concerns the right to move without being traced.[403]

From an ECHR perspective, it is important to note the case of *Shimovolos v Russia*.[404] The case concerned the applicant having their name stored on a 'Surveillance Database.' Whenever a person on this database decided to travel, the Department of Transport would be notified.[405] The ECtHR noted that the Surveillance Database which allowed the collection of the *applicant's movements within Russia* interfered with their private life,[406] and violated it (author's emphasis).[407] What is of importance here is that once the ECtHR found a violation of Article 8, they, of their own motion (likely through Rule A1(1)),[408] asked whether having the applicant's *name* in the Surveillance Database violated Article 2 Protocol 4.[409] The ECtHR concluded that based on a finding of violation of Article 8, although the point was admissible, no separate issue arose under Article 2 Protocol 4.[410] This acknowledges the interplay between Article 8 and Article 2 Protocol 4, in which either or both may be examined depending on the circumstances of the case.[411] This, therefore, highlights that the ECtHR are prepared to accept that storing data on movements may engage Article 2 Protocol 4, which would fall in line with the RCC.

To strengthen the engagement of Article 2 Protocol 4, location data will be considered. Blumberg and Eckersley regard locational privacy as 'the ability of an individual to move in public space with the expectation that under normal circumstances their location *will not be systematically and secretly recorded* for later use (author's emphasis).'[412] However, the ECtHR in *Uzun v Germany*[413] distinguished GPS surveillance from visual and acoustical surveillance because the latter 'disclose[s] more information on a person's conduct, opinions or feelings.' It is contended that the ECtHR are mistaken in this context. As noted before Dr Alex Pentland highlighted that just 'by watching where you spend time, I can say a lot about the music you like, the car you drive, your financial risk, your risk for diabetes.'[414] Furthermore, it was already

[399] *Digital Rights Ireland Ltd*, (n396), [78].
[400] Lilian Mitrou, 'The impact of communications data retention on fundamental rights and democracy – the case of the EU Data Retention Directive in Kevin D. Haggerty and Minas Samatas (ed) *Surveillance and Democracy* (Routledge and Cavendish 2010), 134.
[401] Lilian Mitrou, (n109), 429.
[402] Michael Levi and David S. Wall, 'Technologies, Security, and Privacy in the Post-9/11 European Information Society' (2004) Journal of Law and Society 31:2 194, 206.
[403] Lilian Mitrou, (n400), 134.
[404] *Shimovolos v Russia* App no. 30194/09 (ECHR, 21 June 2011).
[405] ibid, [6-7].
[406] ibid, [66].
[407] ibid, [71].
[408] Rules of Court (14 November 2016) <http://www.echr.coe.int/Documents/Rules_Court_ENG.pdf> accessed 11 November 2017.
[409] *Shimovolos*, (n404), [72].
[410] ibid, [73].
[411] *Nachova and Others v Bulgaria* App nos. 43577/98 and 43579/98 (ECHR, 6 July 2005), [161].
[412] Andrew J. Blumberg and Peter Eckersley, 'On Locational Privacy, and How to Avoid Losing it Forever' (August 2009) <https://www.eff.org/files/eff-locational-privacy.pdf> accessed 13 May 2017, p1.
[413] *Uzun v Germany* App no. 35623/05 (ECHR, 2 September 2010), [52].
[414] Robert Lee Hotz, 'The Really Smart Phone' *Wall Street Journal* (New York City, 23 April 2011) <https://www.wsj.com/articles/SB10001424052748704547604576263261679848814> accessed 14 April 2017.

noted that location data can reveal a person's religion and Blumberg and Eckersley has noted how *location databases* can reveal very sensitive information.[415] The then (and first) Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, noted that surveillance impacts upon various rights *including* freedom of movement because they all require 'privacy to be able to develop effectively.'[416] Scheinin continued that freedom of movement is *substantially* affected by surveillance because the 'creation of secret watch lists, *excessive data collection* and sharing and imposition of intrusive scanning devices or biometrics, *all create extra barriers to mobility* (author's emphasis).'[417]

It becomes clear that data retention interferes with freedom of movement that is protected by Article 2 Protocol 4. There is, however, a caveat, with regards to the UK. The UK signed Article 2 Protocol 4 on 16 September 1963, but did not *ratify* it. Therefore, the ECtHR would not have jurisdiction to consider it.[418] However, ratification is not necessary for it will be sufficient 'that the relevant international instruments denote a continuous evolution in the norms and principles applied in international law.'[419] There are many international law principles governing freedom of movement, from the Article 13 of the Universal Declaration of Human Rights (UDHR), Article 12 International Covenant on Civil and Political Rights (ICCPR), and Directive 2004/38/EC. This allows Article 2 Protocol 4 to be applied to rights that have been ratified and can be enforced in the UK indirectly.[420] It has already been noted that Article 2 Protocol 4 interlinks with Article 8 in terms of data retention. Freedom of movement has also been linked with Articles 9,[421] 11[422] and 10.[423] It has already been established that data retention interferes with each of these Convention Rights which only serves to strengthen their links with Article 2 Protocol 4. The European Parliament's Directorate General noted that the digital applications of freedom of movement and *the right to counsel* has not been sufficiently explored.[424] The latter point is important considering that Martin Scheinin highlighted that surveillance can have an impact on due process rights,[425] and for that reason it is necessary to consider Article 6.

4.10 Article 6 ECHR

(a) Relevant Provisions of Article 6

[415] Andrew J. Blumberg and Peter Eckersley, (n412), p1-2.
[416] Martin Scheinin, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism' A/HRC/13/37 (28 December 2009) <http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf> accessed 14 May 2017, para 33.
[417] ibid, para 37.
[418] *Ismail DUYGULU v Turkey* App no. 4667/03 (ECHR, 20 November 2007), [2].
[419] *Demir and Baykara v Turkey* App no. 34503/97 (ECHR, 12 November 2008), [85-6].
[420] Matthew White, 'When can EU citizens be expelled from the UK after Brexit? The Human Rights Dimension' (4 October 2016) <https://eulawanalysis.blogspot.co.uk/2016/10/when-can-eu-citizens-be-expelled-from.html> accessed 14 May 2017.
[421] *Cyprus v Turkey* App no. 25781/94 (ECHR, 10 May 2001), [241-7].
[422] ibid, [364-371].
[423] *Djavit v Turkey* App no. 20652/92 (ECHR, 20 February 2003), [38-9].
[424] European Parliament, 'Surveillance and censorship: The impact of technologies on human rights' (2015) <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf> accessed 14 May 2017, p12.
[425] Martin Scheinin, (n416), para 38.

It has highlighted that 'the respect for private correspondence under Article 8 relate either directly or indirectly to the right to a fair trial.'[426]The relevant provisions of Article 6 in relation to data retention are Article 6(1), (2) and 3(c) which respectively provide for in the determination of one's civil rights and obligations or any criminal charge against them, everyone is entitled to a fair trial, presumption of innocence and the right to effective legal assistance. This is loosely similar to Article's 47/8 of the CFR.

(b) Does Surveillance Engage Article 6?

The question of whether surveillance engages Article 6 was first dealt with in *Klass*, in which the ECtHR ruled even if it were, it was not violated.[427] The reasoning was that due to the very secretive nature of surveillance i.e. subject not knowing, they were incapable of initiating *a priori* judicial control, which, therefore, escapes the requirements of Article 6.[428] However, in *Kennedy v UK*, the ECtHR were reluctant to answer the question as to whether Article 6 applies to surveillance measures, instead acting on the assumption that it did based on the IPT's reasoning of what constitutes a civil right, which did not in fact violate Article 6.[429] This has been severely criticised by JUSTICE for departing from *Klass* as Article 6 'can only be [engaged] once a person has been notified of a surveillance decision that the requirements of a fair hearing come into play.'[430] Grace has suggested that engaging and interfering with Article 8 'ensures that the requirement of the determination of the civil rights of the 'subject' is met in terms of subsequently engaging Article 6.'[431] This, therefore, proceeds on the assumption that surveillance measures such as data retention engages Article 6, in which the two other requirements, presumption of innocence and the right to effective legal assistance will need to be considered.

(c) Data Retention and the Presumption of Innocence: Rethinking 'Criminal Charge'?

The presumption of innocence is one of the fundamental principles governing criminal law procedure and is included in all the most important international documents of human rights.[432] The first linking of presumption of innocence and data retention (concerning DNA and fingerprint data) came from the GC in *S and Marper v UK*. The GC noted that it:

> [I]s true that the retention of the applicants' private data cannot be equated with the voicing of suspicions. *Nonetheless, their perception that they are not being treated as innocent* is heightened by the fact that *their data are retained indefinitely in the same*

[426] Bart van der Sloot, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"' (2015) Utrecht Journal of International and European Law 31:80 25, 30.
[427] *Klass*, (n13), [75].
[428] ibid.
[429] *Kennedy v UK* App no. 26839/05 (ECHR, 18 May 2010), [179].

[430] JUSTICE, 'Freedom from Suspicion Surveillance Reform for a Digital Age' (October 2011) <http://www.statewatch.org/news/2011/nov/uk-ripa-justice-freedom-from-suspicion.pdf> accessed 04 October 2016, para 379.
[431] Jamie Grace, 'Clare's Law, or the national Domestic Violence Disclosure Scheme: the contested legalities of criminality information sharing' (2015) The Journal of Criminal Law, 79:1, 36.
[432] Jonida Milaj and Jeanne Pia Mifsud Bonnici, 'Unwitting subjects of surveillance and the presumption of innocence' (2014) Computer Law and Security Review 30:4 419, 421.

> *way as the data of convicted persons*, *while the data of those who have never been suspected of an offence are required to be destroyed* (author's emphasis).[433]

The risk of stigmatisation[434] highlights that the GC had concerns with the retention of data (albeit indefinite) of those who were only ever suspected and never convicted, a presumption of guilt.[435] Additionally, crucially, it highlights that those who were never suspected, their data has to be destroyed. From a communications data retention perspective, however, this is not the case as it marked a swing from a post-crime to a pre-crime society, based on risk assessment, suspicion and pre-emption.[436] As Mariuca Morariu notes, it is this 'preemptive action where condemnation occurs first before the search for proof commences…that inflicts heavy losses on civil liberties.[437]

This was highlighted by the RCC where they noted that data retention applies to all, regardless of whether they have committed crimes or not or whether they are the subject of an investigation or not. For the RCC, this would likely to overturn the presumption of innocence and to transform a priori all users of electronic communications technology into people susceptible of committing terrorism crimes or other serious crimes.[438]

The CJEU in *Digital Rights Ireland* and in *Tele2 and Watson* also picked up on the fact that the DRD did not require any relationship between the data whose retention is provided for and a threat to public security.[439] However, for the presumption of innocence to apply, an individual has to be 'charged' with a 'criminal offence.' The terms 'criminal charge' and 'charged with a criminal offence' in Articles 6(1) and (2) respectively have the same meaning.[440] Under Article 6 'criminal charge' has an autonomous meaning and not confined to national categorisations.[441] A 'charge' could be defined as the 'official notification given to an individual by the competent authority of an allegation that he has committed a criminal offence' or whether 'the situation of the [suspect] has been substantially affected.'[442] Regarding the 'criminal' aspect of Article 6, the ECtHR has developed certain criteria to assess applicability based upon:

1. classification in domestic law;
2. nature of the offence; and
3. severity of the penalty that the person concerned risks incurring.[443]

Therefore, the question becomes, would data retention trigger the 'criminal charge' aspect of Article 6(2) for the presumption of innocence to apply? Thomas and Geert take the restrictive view that the presumption of innocence applies only as a procedural safeguard once a specific

---

[433] *S and Marper*, (n28), [122].
[434] ibid; *M.K. v France* App no. 19522/09 (ECHR, 18 April 2013), [42].
[435] Jonida Milaj and Jeanne Pia Mifsud Bonnici, (n432), 420.
[436] ibid, 419.
[437] Mariuca Morariu, 'How secure is to remain private? On the controversies of the European Data Retention directive' (2009), Amsterdam Social Science 1:2 46, 50.
[438] Romania Constitutional Court, (n19).
[439] *Digital Rights Ireland*, (n189), [59]; *Tele2 Sverige AB and Watson*, (n193), [106].
[440] Council of Europe, 'Guide on Article 6 of the European Convention on Human Rights - – Right to a fair trial (criminal limb)' (2014) <http://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf> accessed 15 May 2017, para 9.
[441] *Adolf v Austria* App no. 8269/78 (ECHR, 26 March 1983), [30].
[442] *Deweer v Belgium* App no. 6903/75 (ECHR, 27 February 1980), [46]; *Eckle v Germany* App no. 8130/78 (ECHR, 15 July 1982), [73]; *McFarlane v Ireland* App no. 31333/06 (ECHR, 10 September 2010), [143].
[443] *Engel and Others v UK* App nos. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72 (ECHR, 8 June 1976), [82-3].

crime has been attributed to an individual.[444] However, Alwin Van Dijk has argued that 'any *act* that might convey to a reasonable actor *that he is not presumed innocent* of a punishable offence constitutes a [presumption of innocence] interference (author's emphasis).'[445] Importantly, Alwin Van Dijk gives the example of wire-tapping as an example of presumption of innocence interference.[446] Jonida Milaj and Jeanne Pia Mifsud Bonnici, however, note that ECtHR jurisprudence cannot meet the extensive requirement of Van Dijk because the application of presumption of innocence is 'linked with a specific criminal proceeding' and thus would not apply to individuals whom mass surveillance treats as general suspects.[447]

Despite this, Milaj and Bonnici contend that mass surveillance undermines the operation of the principle as a procedural safeguard through the stages of a criminal process.[448] Milaj and Bonnici refer to the European Parliament's recognition of the relationship between mass surveillance and the presumption of innocence.[449] It is important to note that the European Parliament were aware that these surveillance programmes were another step 'towards the establishment of a fully-fledged preventive state…often not in line with… the presumption of innocence.'[450] As Antonella Galetta states, the criminal justice process usually consists of several consequent states from the presumption of innocence to investigation, evidence collection, charge, trial, guilty verdict and punishment.[451] The, preventative state, however, is the antithesis of this. We are not quite in Minority Report territory yet, but the foundations for it are being laid out.

Katerina Hadjimatheou has articulated on several occasions that surveillance does not necessarily undermine the presumption of innocence[452] and the 'least costly morally and most efficient when used as a means of enforcing the rules of a specific activity or institution.'[453] But this line of reasoning would forego any need to deduce grounds of suspicion[454] and does not fully consider the chilling effect it creates irrespective of the legality and morality of behaviour, nor the lack of specificity of activities that 'justify' surveillance. Further, it does not consider that some forms of untargeted surveillance are just as if not more intrusive than targeted surveillance.[455] Moreover, Milaj and Bonnici highlight several reasons why mass surveillance (which is relevant to data retention)[456] threatens the presumption of innocence because:

---

[444] Jonida Milaj and Jeanne Pia Mifsud Bonnici, (n432), 422; see references to Weigend Thomas, 'There is only one presumption of innocence' (2013) Neth J Leg Philos 42:3 193 and Knigge Geert, 'On presuming innocence' (2013) Neth J Leg Philos 42:3 225.
[445] Alwin A. van Dijk, 'Retributivist Arguments against Presuming Innocence' (2013) Neth J Leg Philos 42:3 249, 250.
[446] ibid, fn3.
[447] Jonida Milaj and Jeanne Pia Mifsud Bonnici, (n432), 422.
[448] ibid, 423.
[449] ibid.
[450] European Parliament resolution of 12 March 2014, (n189), para 12, see also para 10 and 20.
[451] Antonella Galetta, (n2).
[452] Katerina Hadjimatheou, 'Surveillance Technologies, Wrongful Criminalisation, and the Presumption of Innocence' (2016) Philosophy & Technology <http://wrap.warwick.ac.uk/79568/1/WRAP_art%253A10.1007%252Fs13347-016-0218-2_.pdf> accessed 16 May 2017.
[453] Katerina Hadjimatheou, 'The Relative Moral Risks of Untargeted and Targeted Surveillance' (2014) Ethic Theory Moral Prac 17 187.
[454] *Roman Zakharov v Russia* App no. 47143/06 (ECHR, 4 December 2015), [260].
[455] See Chapter 3.
[456] Jonida Milaj and Jeanne Pia Mifsud Bonnici, (n432), 425.

1. mass surveillance places significant personal information in the hands of authorities, in which the individual is unaware,
2. information could be gathered when an individual was not a suspect and subsequently used against them potentially making it un-rebuttable,
3. this leads to a *de facto* overturning the burden of proof[457] during the stages of a criminal process from the accuser to the accused;
4. due to the lack of transparency and the information asymmetry between the accuser and the accused, the presumption of innocence can no longer serve anymore as a procedural safeguard for the individual in the mass surveillance era.[458]

Antonella Galetta adds to this by noting that pre-crime surveillance creates distrust between citizen and the state,[459] though Katerina Hadjimatheou believes there is a lack of evidence supporting this.[460] But this trust is implicitly linked with the chilling effect of the exercise of rights, which *has* been well evidenced. Galetta not only highlights the link between the presumption of innocence and the reputational aspect of Article 8, but the dual dimension of Article 6(2), the legal and moral presumption of innocence.[461] Galetta uses *S and Marper* and the risk of stigmatation the ECtHR elucidated to as a basis to argue that the ECtHR 'recognises that the presumption of innocence does not only give rise to a human right but also to a moral value that should be safeguarded.'[462] Galetta concludes a clear stance from the ECtHR expanding the scope of presumption of innocence is desirable as this would keep pace with society as the 'law must mirror societal developments and provide answers to social needs.'[463] Galetta makes note of the '[l]iving law' as the highest expression of the synthesis between law and society.'[464]Such a position is entirely feasible considering that the ECHR is 'living instrument' in which it must be interpreted in the light of present-day conditions.'[465]

Additionally, a criminal charge under Article 6(2) could be engaged by the substantial effect it has on an individual. Throughout this Chapter, it has been noted how data retention not only interferes with but chills the exercise of fundamental rights. Furthermore, in *Barry v Ireland* the ECtHR concluded that once a search warrant had been issued and executed on the applicant's premises, it amounted to a charge within the meaning of Article 6.[466] In *Romanova v Russia* the ECtHR considered the possibility of searches *and* secret surveillance substantially affecting the applicant (thus amounting to a charge) and only declined to do so because neither party made submissions on that matter.[467] This implies that secret surveillance can also substantially affect someone within the meaning of Article 6(2). Data retention has been

[457] See also Gary T. Marx, *Undercover: Police Surveillance in America* (University of California Press, Berkeley 1989); Gary T. Marx, 'Seeing Hazily, But Not Darkly, Through the Lens: Some Recent Empirical Studies of Surveillance Technologies' (2005) Law and Social Inquiry, 30:2 339.
[458] Jonida Milaj and Jeanne Pia Mifsud Bonnici, (n432), 425.
[459] Antonella Galetta, (n2).
[460] Katerina Hadjimatheou, 'Surveillance, the moral presumption of innocence, the right to be free from criminal stigmatisation and trust' (2013) <https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D4.5-Surveillance-the-moral-presumption-of-innocence.pdf> accessed 16 May 2017, p25.
[461] Antonella Galetta, (n2).
[462] ibid.
[463] ibid.
[464] ibid.
[465] *Tryer v United Kingdom* App no. 5856/72 (ECHR, 25 April 1978), [31].
[466] *Barry v Ireland* App no. 18273/04 (ECHR, 15 December 2005), [33-5].
[467] *Romanava v Russia* App no. 23215/02 (ECHR, 11 October 2011), [138].

likened to 'fishing'[468] exercises which is designed to bring in information,[469] similar to a search. Moreover, data retention is a form of secret surveillance,[470] and due to the fact that one's property and devices within it will in future likely to be connected to the Internet via the Internet of Things (IoT),[471] any retention of data substantially affects the individual involved for the purposes of Article 6(2). Therefore, taking into account the GC's concern in *S and Marper*, the RCC assertion regarding data retention, the CJEU acknowledging data retention not distinguishing between suspects, the arguments made by Milaj, Bonnici, Galetta, the position on substantially affected person and the ECHR being a 'living instrument,' it is in the author's opinion that data retention does trigger Article 6(2) and therefore the presumption of innocence should apply. The presumption of innocence has been closely linked with the right to not incriminate oneself.[472]

(d) Self Incrimination

Chapter 6 discusses whom the obligation to retain can be imposed on. It will be demonstrated that this can include 'home grown'[473] communications data as well as commercial. Conrad Fischer notes that when communications data in the systems of end users i.e. Skype, private mail servers are regarded as legal communications data, therefore eligible for retention, the inevitably of privilege against self-incrimination applies.[474] In *Saunders v UK*, the ECtHR noted that the right to not incriminate oneself is primarily concerned with respecting the will of an accused to remain silent but does not extend to compulsory powers such as measures issued by warrants, breath and blood samples etc.[475] Fischer notes that self-incrimination only applies to the active cooperation of the accused in which he notes that 'an obligation to retain and disclose home grown private traffic data as a form of forced active cooperation.'[476] As Smith noted, customers or other third parties could be obliged to generate data to be retained.[477]

Furthermore, the previous Chapter noted that passwords are a type of communications data. In *S & Anor, R* the English and Welsh Court of Appeal (CoA) acknowledged that privilege against self-incrimination *may* be engaged by a requirement of disclosure of knowledge of the means of access to protected data under compulsion of law.[478] The fact that passwords amount to communications data for retention discloses them.

Self-incrimination also raises issues with regards to neurotechnologies (mentioned above) because as Ienca and Andorno note, it becomes a question of:

---

[468] Franziska Boehm and Paul de Hert, *The rights of notification after surveillance is over: ready for recognition?* (Yearbook of the Digital Enlightenment Forum, IOS Press 2012), pp. 19-39.
[469] *Kopp v Switzerland* App no. 23224/94 (ECHR, 25 March 1998), Judge Pettit's concurring opinion; Stephen Uglow, 'The Human Rights Act 1998: Part 4: covert surveillance and the European Convention on Human Rights,' Criminal Law Review [1999] 287, p289.
[470] See Chapter 5.
[471] See Chapter 6.
[472] *Saunders v UK* App no. (ECHR, 17 December 1996), [68].
[473] Conrad Fischer, 'Communications Network Traffic Data' (2010) <http://alexandria.tue.nl/extra2/689860.pdf> accessed 17 May 2017, p188.
[474] ibid.
[475] *Saunders*, (n472), [69].
[476] Conrad Fischer, (n473), p189-190.
[477] Graham Smith, 'Illuminating the Investigatory Powers Act' (22 February 2018) <https://www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html> accessed 6 June 2018.
[478] *S & Anor, R v* [2008] EWCA Crim 2177, [24].

> [W]hether the mere record of thoughts and memories without any coerced oral testimony or declaration is evidence that can be legally compelled, or whether this practice necessarily requires the 'will of the suspect' and therefore constitutes a breach of the privilege against forced self-incrimination.[479]

There is a risk that people may be protected against self-incriminatory statements, but not their thoughts[480] a 'self-incrimination may now occur *silently* just as aloud (author's emphasis).'[481]

(e) Effective Legal Assistance

Bernal notes that surveillance can interfere with the legal process in many ways, one of which is the interference with the lawyer's correspondence with their clients.[482] A person must be able to, without constraint, consult a lawyer whose profession involves giving independent legal advice to all who need it.[483] This demonstrates the link with the correspondence aspect Article 8.[484] The ECtHR has noted that the accused's rights to communicate with his advocate out of hearing of a third person *is part of the basic requirements of a fair trial in a democratic society* and follows from Article 6(3)(c). Moreover, if a lawyer is unable to confer with his client and receive confidential instructions from him without surveillance, his assistance loses much of its usefulness whereas the Convention is intended to guarantee rights that are practical and effective.[485] Any *limitation on relations between clients and lawyers, whether inherent or express*, should not thwart the effective legal assistance to which a defendant is entitled.[486] Additionally, *any* interference with privileged material 'should be exceptional, be justified by a pressing need and will always be subjected to the strictest scrutiny (author's emphasis).'[487]

From a UK perspective, in *Re McE*,[488] the House of Lords discussed legal professional privilege (LPP), surveillance and Article 6(3)(c). When referring to ECtHR case law, Lord Carswell noted 'the effect of the supervision, not the supervision in itself, which brought about the breach'[489] of Article 6. Lord Neuberger highlighted that:

> [I]t is self-evident that knowing that a consultation or the communication may be the subject of surveillance could have a chilling effect on the openness which should govern communications between lawyer and client.[490]

The Law Society and the Bar Council (the professional bodies representing barristers and solicitors in England and Wales) raised concerns about data retention and LPP.[491] They note

---

[479] Marcello Ienca and Roberto Andorno, (n295), 17.
[480] ibid.
[481] Nita A. Farahany, 'Incriminating Thoughts' (2012) Stanford Law Review 64 351, 407.
[482] Paul Bernal, (n4), 255-6.
[483] Case C-155/79 *AM & S Europe Limited v Commission of the European Communities Legal privilege* [1982] ECR I-01575, [18].
[484] *McE, Re* (Northern Ireland) [2009] UKHL 15, [6].
[485] *S. v Switzerland* App nos. 12629/87 13965/88 (ECHR, 28 November 1981), [48]; *Brennan v UK* App no. 39846/98 (ECHR, 16 October 2001), [58].
[486] *Sakhnovskiy v Russia* App no. 21272/03 (ECHR, 2 November 2010), [102].
[487] *Khodorkkovsky and Lebedev v Russia* App nos. 11082/06 and 13772/05 (ECHR, 25 July 2013), [627].
[488] *McE,* (n484).
[489] ibid, [84].
[490] ibid, [111].
[491] Law Society and Bar Council, 'Investigatory Powers and Legal Professional Privilege' (2015) <https://www.lawsociety.org.uk/news/documents/position-paper-investigatory-powers-legal-professional-privilege-october-2015/> accessed 17 May 2017.

that the problem with bulk communications data retention is that it does not prevent LLP data from entering the 'pool' in the first place,[492] something which the Council of Bars and Law Societies of Europe (CCBE)[493] and the CJEU highlighted.[494] The Law Society and Bar Council considered that 'new legislation should prevent an obligation being placed on service providers *to retain data relating to communications to or from users known to be professional legal advisers* (author's emphasis).'[495] This was also the position of AG Saugmandsgaard Øe in *Tele2 and Watson*.[496] Jessica Sobey notes that '[k]nowing who a lawyer contacts, when the contact was made and even where the point of contact was in geographical terms at the time, can be enough to represent a material breach of privilege.'[497] Thus, this could have the chilling effect Lord Neuberger highlighted, not only undermining Article 6(3)(c), but also Article 6(1),[498] correspondence under Article 8, but also the professional aspect of private life, and ultimately striking at the freedom of communication between lawyer and client. The pertinent points of failing to discriminate data retention practices leads to the final Convention Right for consideration, Article 14.

4.11 Article 14 ECHR

Article 14 sets out that:

> The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

Unlike Article 1 Protocol 12,[499] Article 14 is not freestanding,[500] therefore, having no independent existence.[501] For this reason it has been regarded as odd,[502] parasitic,[503] Cinderella-

---

[492] ibid, para 32.
[493] The Council of Bars and Law Societies of Europe, 'Comments on the Draft Framework Decision On the Retention of Data' (February 2005) <http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/lobbying_paper_data_1_1182260611.pdf> accessed 12 November 2017, p2. The CCBE represents through its member bars and law societies more than 700,000 lawyers.
[494] *Digital Rights Ireland*, (n189), [57-8]; *Tele2 Sverige AB and Watson*, (n193), [105].
[495] Law Society and Bar Council, (n491), para 32.
[496] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-572, Opinion of Saugmandsgaard Øe, [212].
[497] Jessica Sobey, 'Legal professional privilege under fire' <http://www.stokoepartnership.com/wp-content/uploads/2016/06/Jessica-Sobey-Legal-Professional-Privilege-Under-Fire-CLJ-Vol.-180.pdf> accessed 17 May 2017.
[498] *Khodorkkovsky and Lebedev*, (n487), [629].
[499] General prohibition of discrimination. 1 The enjoyment of any right set forth by law shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. 2 No one shall be discriminated against by any public authority on any ground such as those mentioned in paragraph 1.
[500] *Airey v Ireland* App no. 6289/73 (ECHR, 9 October 1979), [30].
[501] *Chassagnou v France* App nos. 25088/94, 28331/95 and 28443/95 (ECHR, 29 April 1999), [89]; *Oršuš and Others v Croatia* App no. 15766/03 (ECHR, 16 March 2010), [144].
[502] Janneke Gerards, 'The Discrimination Grounds of Article14 of the European Convention on Human Rights' (2013) Human Rights Law Review 13:1 99, 100.
[503] Joan Small, 'Structure and Substance: Developing a Practical and Effective Prohibition on Discrimination under the European Convention on Human Rights' (2003) International Journal of Discrimination and the Law 6 45, 47; Aaron Baker, 'The Enjoyment of Rights and Freedoms: A New Conception of the 'Ambit' under Article 14 ECHR' (2006) MLR 69:5 714, 715;

esque,[504] and weak.[505] However, when the ECtHR has noted that when Article 14 is considered to have a fundamental aspect to the case, it will be considered,[506] even where there has been no violation of the substantive right.[507] Article 14 requires there to be a difference in treatment of persons in analogous, or relevantly similar, situation, it need not be identical.[508] For the ECtHR, '*the principle of non-discrimination* between individuals as regards their enjoyment of public freedoms, *which is one of the fundamental principles of democracy* (author's emphasis).'[509]

Due to the indiscriminate nature of data retention, it is difficult to rely on anything within Article 14 other than 'other status,' which is described as personal status.[510] This has often been interpreted 'very widely' be the ECtHR and would seem 'that almost any distinction within the ambit of a Convention right can trigger an Art 14 inquiry.'[511] Data retention raises indirect discrimination aspects of Article 14. The GC in *D.H. and Others v the Czech Republic*[512] noted that:

> [A] difference in treatment may take the form of disproportionately prejudicial effects of a general policy or measure which, though couched in neutral terms, discriminates against a group…may amount to "indirect discrimination", which does not necessarily require a discriminatory intent.

On the specifics of DNA data retention, Sedley LJ in the CoA considered Article 14 in the aspect of indirect discrimination.[513] Sedley LJ noted that central to 'indirect discrimination is the ostensibly *neutral factor* which on analysis significantly and unjustifiably disadvantages a protected group (author's emphasis).'[514] Sedley LJ continued that '[t]o take as your pool simply the group which asserts that it is being discriminated against and to find – as you practically always will – *that they are all being treated the same is to defeat the rationale of indirect discrimination* (author's emphasis).'[515] Sedley LJ concluded that the legal issue is one of 'discrimination between legally innocent people who respectively have and have not been investigated.'[516] Although on appeal to the House of Lords (HoL) in which Lord Steyn rejected Sedley LJ's position,[517] it was noted that 'there is a material distinction between individuals who have had their fingerprints and samples lawfully taken in consequence of being charged with a recordable offence *and those who have not* (author's emphasis).'[518] The GC in *S and Marper*, unfortunately declined to express a view after finding a violation of Article 8.[519]

---

[504] Rory O'Connell, 'Cinderella comes to the Ball: Art 14 and the right to non-discrimination in the ECHR' (2009) Legal Studies 29:2 221.
[505] Verena Zöller, 'Liberty Dies by Inches: German Counter-Terrorism Measures and Human Rights' (2004) German Law Journal 5:5 469, 488.
[506] *Chassagnou*, (n501), [89]; *Oršuš and Others*, (n501), [144].
[507] *Sommerfield v Germany* App no. 31871/96 (ECHR, 8 July 2003), [84].
[508] *Clift v UK* App no. 7205/07 (ECHR, 13 July 2010), [66].
[509] *Refah Partisi (The Welfare Party) and Others v Turkey* App nos. 41340/98, 41342/98, 41343/98 and 41344/98 (ECHR, 13 February 2003), [119].
[510] *Carson and Others v UK* App no. 42184/05 (ECHR, 16 March 2010), [70].
[511] Rory O'Connell, (n504), 222.
[512] *D.H. and Others v the Czech Republic* App no. 57325/00 (ECHR, 13 November 2007), [184].
[513] *Marper & Anor, R (on the application of) v Chief Constable of South Yorkshire & Anor* [2002] EWCA Civ 1275, [89].
[514] ibid, [90].
[515] ibid, [91].
[516] ibid.
[517] *LS, R (on application of) v South Yorkshire Police (Consolidated Appeals)* [2004] UKHL 39, [52].
[518] ibid, [53].
[519] *S and Marper*, (n28), [129].

However, in *RJM*, in Lord Walker's leading judgment, noting there are two types of 'personal characteristics,' i.e. personal/other status, those that are intimate, and importantly those that 'are more concerned *with what people do*, *or with what happens to them* (author's emphasis).'[520] It is this idea of what people do and what is done to them which would make having ones data retained subject to the application of 'other status.' The status of being presumed innocent, and more importantly, not under any suspicion of wrong doing. This would of course be somewhat consistent with the ECtHR's position of not confining other status to the 'sense of being immutable or innate to the person.'[521] Therefore, for the purposes of communications data retention, it has been noted throughout this Chapter that Articles 6, 8-11 and Article 2 Protocol 4 apply, similarly Article 14 would therefore be applicable.

Data retention fails to discriminate between suspects and non-suspects, the legal profession and journalism etc. In *Thlimmenos v Greece*[522] the GC found that refusing to admit an individual to a profession because of a criminal conviction amounted to a violation of Article 14 in conjunction with Article 9 where that conviction was due to conscientious objection. Importantly, the GC noted that:

> The right not to be discriminated against in the enjoyment of the rights guaranteed under the Convention is also violated when States without an objective and reasonable justification *fail to treat differently persons whose situations are significantly different* (author's emphasis).[523]

This is why Article 14 becomes fundamental to the aspect of communications data retention. Data retention as currently envisioned does not distinguish between suspects and non-suspects, it does not take into consideration parts of society whose communications data require special protection. AG Saugmandsgaard Øe in *Tele2 and Watson* thought it desirable that data *such as* those subject to LLP or which makes it possible to identify journalist source should be excluded from data retention obligations.[524]

There is also an issue regarding Big Data retention.[525] There is a clear bias in Big Data to be retained as could be based on what telecommunications are obligated to generate for law enforcement (due to ethnic profiling,[526] which can intensify ethnic profiling)[527] or inherent

---

[520] *RJM, R (On The Application of) v Secretary of State For Work and Pensions* [2008] UKHL 63, [5].
[521] Oddny Mjöll Arnardóttir, 'The Differences that Make a Difference: Recent Developments on the Discrimination Grounds and the Margin of Appreciation under Article 14 of the European Convention on Human Rights' (2014) HRLR 14:4 647, 659.
[522] *Thlimmenos v Greece* App no. 34369/97 (ECHR, 6 April 2000).
[523] ibid, [44].
[524] Opinion of Saugmandsgaard Øe, (n496), [212].
[525] See Chapter 3.
[526] *Gillan and Quinton v UK*, (n389); *S and Marper*, (n28), [38-40] and [124]; Bart van der Sloot, Dennis Broeders and Erik Schrijvers, *Exploring the Boundaries of Big Data* (Amsterdam University Press, Amsterdam 2016), 125; Bernard E. Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* (Chicago: University of Chicago Press 2007); Olivier De Schutter and Julie Ringelheim, 'Ethnic Profiling: A Rising Challenge for European Human Rights Law' (2008) Modern Law Review 71:3 358; Open Society Initiative, 'Equality under Pressure: The Impact of Ethnic Profiling' (2013) <https://www.opensocietyfoundations.org/sites/default/files/equality-under-pressure-the-impact-of-ethnic-profiling-netherlands-20131128_1.pdf> accessed 19 October 2017; Leanne Weber and Ben Bowling, *Stop and Search: Police Power in Global Context* (Routledge 2012); Bart Custers, Tal Zarsky and Bart Schermer, *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases (Studies in Applied Philosophy, Epistemology and Rational Ethics)* (Springer, Heidelberg 2013).
[527] Bart van der Sloot, Dennis Broeders and Erik Schrijvers, *Exploring the Boundaries of Big Data* (Amsterdam University Press, Amsterdam 2016), 125; Joanne P. van der Leun and Maartje A.H. van der Woude, 'Ethnic

within the operations of the telecommunications operators.[528] Biases[529] based on race,[530] (a point the ECtHR has previously acknowledged)[531] gender and socio-economic background[532] would all fall under the ambit of Article 14. This relates to what Lyon describes surveillance as 'social sorting.' He continues that it 'classifies and categorizes relentlessly, on the basis of various – clear or occluded – criteria' and [i]t is often, but not always, accomplished by means of remote networked databases whose algorithms enable digital discrimination to take place.'[533] Such surveillance can create a chilling effect on the freedom of expression of ordinary citizens and a wide range of vulnerable groups.[534] Penney's research has suggested that women and younger people are more likely to be chilled and are less likely to take steps to defend themselves from regulatory actions and threats.[535] It has also been statistically demonstrated that Muslim-American's change their behaviour due to government surveillance fears.[536] This also demonstrates that 'other status' need not be solely relied upon in this regard as Article 14 covers amongst other things as race, colour, sex and religion.

What is also important in regards to 'other status' is that the GC acknowledges that one's place of residence constitutes an aspect of personal status for the purposes of Article 14.[537] Article 14 can also be linked with Article 8-11 and Article 2 Protocol 4 in that discrimination deters and inhibits self-fulfilment as it will prevent 'people from expressing themselves freely due to the fear of how others or society will react.'[538] This is particularly true in the surveillance

---

profiling in the Netherlands? A reflection on expanding preventive powers, ethnic profiling and a changing social and political context' (2011) Policing and Society 21:4 444; Open Society Initiative, 'Equality under Pressure: The Impact of Ethnic Profiling' (2013) <https://www.opensocietyfoundations.org/sites/default/files/equality-under-pressure-the-impact-of-ethnic-profiling-netherlands-20131128_1.pdf> accessed 19 October 2017.

[528] Lee Rainie and Janna Anderson, 'Code-Dependent: Pros and Cons of the Algorithm Age' (8 February 2017) <http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/02/08181534/PI_2017.02.08_Algorithms_FINAL.pdf> accessed 19 October 2017, p57; Latanya Sweeney, 'Discrimination in Online Ad Delivery' (28 January 2013) <https://arxiv.org/pdf/1301.6822.pdf> accessed 19 October 2017; Paul Bernal, (n4), 257-258; Stephen Buranyi, 'Rise of the racist robots – how AI is learning all our worst impulses' (8 August 2017) <https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses> accessed 19 October 2017.

[529] Cathy O'Neil, 'The era of blind faith in big data must end' (April 2017) <https://www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end#t-786714> accessed 17 October 2017.

[530] Kate Crawford and Ryan Calo, 'There is a Blind Spot in AI Research' (2016) Nature 538 311, 312; Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, 'Machine Bias' (23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 19 October 2017.

[531] *Gillan and Quinton*, (n389), [85].

[532] Solon Barocas and Andrew D. Selbst, 'Big Data's Disparate Impact' (2016) California Law Review 104 671.

[533] David Lyon, 'Surveillance as social sorting: computer codes and mobile bodies' in David Lyon (ed) *Surveillance as Social Sorting Privacy, risk, and digital discrimination* (Routledge 2003), 8.

[534] David Kaye, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (11 May 2016) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/12/PDF/G1609512.pdf?OpenElement> accessed 4 May 2017, para 57.

[535] Jonathon W. Penney, 'Internet surveillance, regulation, and chilling effects online: a comparative case study' (2017) Internet Policy Review 6:2; Jonathon W. Penney, 'Whose Speech Is Chilled by Surveillance?' (7 July 2017) <http://www.slate.com/articles/technology/future_tense/2017/07/women_young_people_experience_the_chilling_effects_of_surveillance_at_higher.html> accessed 17 August 2017.

[536] Dawinder S. Sidhu, (n285).

[537] *Carson and Others*, (n510), [71]. See Chapter 7.

[538] Sandra Wachter, (n163), p10.

context as being forced to disclose information poses a 'threat to self-fulfilment because it enables discrimination.'[539]

4.12 Conclusions: Article 8 underpinning democracy

This Chapter has highlighted the various ways in which communications data retention interferes with or chills the exercise of various Convention Rights. The starting point was consideration for the most obvious right in question, Article 8 and the various ways in which data retention interfered with this right. Just as van der Hilst noted 'it became apparent that the right to respect for private life, *besides having a value on its own*, *is of instrumental importance to the fulfilment of other rights* (author's emphasis).'[540] The former Independent Reviewer of terrorism legislation David Anderson Q.C., shared a similar view.[541] Wachter echoes what has been argued in this Chapter, that privacy and Article 8 is a necessary precondition for self-development, personal fulfilment and the free enjoyment of fundamental human rights. [542] Wachter continues that Article 8 promotes tolerance, equality and informational self-determination to fight discrimination, and is essential (but not limited to) for the exercise of Article 9-11 rights. [543] This is exacerbated by digital technologies which communications data collection and storage threaten not only Article 8, but 9-11,[544] 6, 14 and Article 2 Protocol 4.

Not only the private life aspect of Article 8, but family life, correspondence become relevant. It has already been seen that privacy and therefore Article 8 is not just an individual value, but a societal one, and ultimately one for democracy. Scheinin has noted that '[t]he right to privacy is therefore not only a fundamental human right, but also a human right that supports other human rights and forms the basis of any democratic society.'[545] There can be no democracy without pluralism,[546] and this Chapter has demonstrated how Article 8 necessitates and *underpins* all of the rights that promote it. For this reason, Wachter strongly argues that privacy must be elevated above other human rights because 'it is the basis for personal development and fulfilment and due to its position as an underlying, enabling requirement for the realisation of other human rights.'[547] In the context of digital technologies, this is certainly within the power of the ECtHR by interpreting the ECHR as a living instrument[548] in creative ways.[549]

The position of Article 8 being a pillar of democracy is also highlighted by the ECtHR where it was noted in *Gorzelik and Others*.[550]The ECtHR's role in the promotion of democracy has been noted,[551] and with that, to promote democracy, the ECtHR must ensure that chilling effects are minimised as:

---

[539] ibid, p10-11.
[540] Rozemarijn van der Hilst, (n374), p27.
[541] David Anderson, 'A Question of Trust, Report of the Investigatory Powers Review' (June 2015) <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf> accessed 12 May 2017, para 2.12.
[542] Sandra Wachter, (n163), p4.
[543] ibid, p4, 8-12.
[544] ibid, p18-20.
[545] Martin Scheinin, (n416), para 11.
[546] Alastair Mowbray, 'Contemporary aspects of the promotion of democracy by the European Court of Human Rights' (2014) European Public Law 20:3 469.
[547] Sandra Wachter, (n163), p21.
[548] ibid.
[549] Alastair Mowbray, 'Creativity of the European Court of Human Rights' (2005) Human Rights Law Review 5:1 57, 79.
[550] *Gorzelik and Others*, (n324), [89].
[551] Alastair Mowbray, (n549).

> The value of protecting against chilling effects is not measured simply by focusing on the particular individuals who are deterred from exercising their rights. Chilling effects harm society because, among other things, they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity.[552]

For this reason, surveillance programmes (including data retention) cannot be reduced to questions of privacy or data protection v security, but have to be framed in terms of collective freedoms and democracy. [553] This, will ultimately lead to the question of what nature, scale and depth of surveillance can be tolerated in and between democracies?[554] Throughout this Chapter, it has been argued that data retention is synonymous with surveillance, the next Chapter will explain why data retention *is* surveillance.

[552] Daniel J. Solove, ''I've Got Nothing to Hide' and Other Misunderstandings of Privacy' (2007) San Diego Law Review 44 745, 746.
[553] European Parliament, 'National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law' (2013) <http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf> accessed 14 November 2017, p5.
[554] ibid, p11.

Chapter 5: Communications Data Retention as Mass Secret Surveillance within Surveillance?

5.1 Introduction

One of the major battle grounds of the data retention debate focusses on whether data retention is surveillance or not, this Chapter seeks to clarify the debate. In this Chapter I will not only argue that data retention is a form of mass secret surveillance (considering past and contemporary measures) by highlighting that Lyon's definition[1] may no longer be adequate. It will also be argued that surveillance should not be normalised whilst also demonstrating that data retention has striking similarities with the Panopticon.[2] In addition to the Panopticon, I will demonstrate that data retention is also Panspectric[3] and would actually be classified as surveillance under national and European law. Finally, in this Chapter I highlight that although the Panopticon is usually associated with State power, it will be demonstrated that the State and private entities work in synergy in which the State allows or mandates them to conduct surveillance for which it can utilise. Hence data retention is also mass secret surveillance *within* surveillance. This will strengthen the argument made in Chapter 3 that the same strict safeguards for interception and secret surveillance should equally apply to data retention.

In 2001, during the debate on Clause 102 of the Anti-terrorism, Crime and Security Bill[4] regarding a provision for mandatory retention of communications data, both Lord Phillips[5] and Earl of Northesk[6] discussed the extent of mass surveillance. Lord Thomas Gresford acknowledged the potential for surveillance 'of every member of the community who uses a mobile telephone or e-mail'[7] and Elizabeth France, the then Data Protection Commissioner noted that this would amount to *disproportionate general surveillance of communications*.[8]

Lord Rooker, however, disagreed believing that the very idea was 'extravagant in the extreme.'[9] Over a decade later similar sentiments were echoed during the debates on what would soon to be the Investigatory Powers Act 2016 (IPA 2016), by the opposition[10] and Government.[11]

(a) An Overview

[1] David Lyon, *Surveillance Studies: An Overview* (Cambridge: Polity Press 2007).
[2] Michel Foucault, *Discipline & Punish* (New York: Vintage 1977).
[3] Irene Maria Portela and Maria Manuela Cruz-Cunha, 'What About the Balance Between Law Enforcement and Data Protection?' in Irene Maria Portela and Maria Manuela Cruz-Cunha (eds) *Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues*, (IGI Global 2010).
[4] HL Deb 4 December 2001, vol 629 cols 787-826.
[5] ibid, col 808.
[6] HL Deb 27 November 2001, vol 629, c251,
[7] HL Deb 4 December 2001, (n4), cols 811-812.
[8] BBC, 'Safeguard over e-mail 'snooping' Bill' *BBC News* (London, 13 July 2000) <http://news.bbc.co.uk/1/hi/uk/830968.stm> accessed 15 November 2017.
[9] HL Deb 4 December 2001, (n4), cols 809-810.
[10] HC Deb 4 November 2015, vol 601, col 973.
[11] ibid, col 975.

In the joined cases C‑203/15 and C‑698/15 (*Tele2 and Watson*),[12] Advocate General (AG) Saugmandsgaard Øe noted similarities between communications data retention and interception. Particularly, the AG made reference to the fact that 'a general data retention obligation will *facilitate equally serious interference* as targeted surveillance measures, including those which *intercept the content of communications* (author's emphasis).'[13] The AG, did not go so far as referring to data retention as mass surveillance,[14] instead regarding it as mass interference affecting a substantial part, if not all of the relevant population.[15] In regards to interception, the European Court of Human Rights (ECtHR) has on more than one occasion observed such a measure as secret surveillance.[16] Although the ECtHR has not yet defined what secret surveillance measures are, it, however, established a link between data retention and surveillance. The contention is that if interception and data retention pose similar levels of interference with fundamental rights (as Chapter 3 demonstrated), and the former being considered a measure of secret surveillance, it will be argued that the latter should also be regarded as secret surveillance. However, before such considerations, it is important to reflect upon previous iterations of data retention.

5.2 Data retention prior to the digital age

The retention of data, is not, however, a new technique made possible because of the advances in technology. Technology has only created a new way to retain and disseminate data. Higgs considers data retention from the period of 1500 to 2000 in England. Higgs argues that one of the main features of a modern Western state which sets it apart from its previous political formations is the central collection and analysis of information, especially that of individuals.[17] Higgs notes that in general terms information is held on citizens in Britain by the modern central state for a limited number of functions such as 'the extraction of taxes; the provision of welfare; the prevention of crime; the general identification of citizens and state employees; and the protection of property rights.'[18] Higgs highlights that what is striking about this list is that such activities were not unknown to pre-modern England nor were they carried out in complete isolation from the central state.[19]

Higgs points out that it was in the twentieth century that 'the citizen body and intellectuals began to grow uneasy at the nature of information gathering by central government, and its perceived threat to civil liberties.'[20] One of such reasons was the impact of new technologies of information handling.[21] Higgs highlights that the database has made access to personal information and its integration much easier.[22] Developed by Herman Hollerith in 1890, and introduced into the British census in 1911, Higgs highlighted the dangers of databases as it was

[12] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-572, Opinion of Saugmandsgaard Øe.
[13] ibid, [254].
[14] Matthew White, 'The new Opinion on Data Retention: Does it protect the right to privacy?' (27 July 2016) < http://eulawanalysis.blogspot.co.uk/2016/07/the-new-opinion-on-data-retention-does.html> accessed 1 November 2016.
[15] Opinion of Saugmandsgaard Øe, (n12), [255-6].
[16] *Roman Zakharov v Russia* App no. 47143/06 (ECHR, 4 December 2015), [229].
[17] Edward Higgs, 'The Rise of the Information State: the Development of Central State Surveillance of the Citizen in England, 1500–2000' (2001) Journal of Historical Sociology 14 :2 175.
[18] ibid, 176.
[19] ibid.
[20] ibid, 188.
[21] ibid.
[22] ibid, 191.

utilised by the Nazi Germany to organise the Holocaust.[23] Higgs continues with the development of 'electronic means of data storage and analysis after the Second World War' which 'allowed these databases to be easily integrated.'[24]

Higgs regards this period as when the British Information State came of age.[25] Fingerprints were one of the pieces of information made available from the Police National Computer (PNC). Throughout his article, Higgs refers to storage, collection and databases of information as surveillance. This Chapter explains why his position is correct. The case *S and Marper v United Kingdom*[26] concerned the indiscriminate retention of DNA and fingerprints, and ruled such activities as incompatible with Article 8 of the ECHR.[27] Brown draws an analogy with DNA/fingerprint retention and communications data retention,[28] because as Brown notes, the ECtHR is not just concerned with the use of data, but its retention. Taking into account Higgs, this begins to highlight that communications data should be considered a form of surveillance. Therefore, it is important to consider just what is regarded as surveillance by experts.

5.3 Surveillance theories and its relationship with data retention

(a) What is Surveillance? Why Lyon's definition may no longer be adequate

Surveillance is said to be rooted in the French verb surveiller translating to 'watch over.'[29] David Lyon, a prominent figure[30] in the discussion on surveillance studies, viewed surveillance as 'the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction.[31] The Oxford dictionary defines it as the close observation, especially of a suspected spy or criminal.[32] According to Lyon, surveillance is focussed when it is orientated towards an individual even when aggregate data may be used in the process. Furthermore, surveillance is systematic when it is intentional, deliberate, and depending on certain protocols and techniques; when it does not happen randomly or spontaneously. Lyon elaborated that surveillance happens when data collection becomes routine. In "societies that depend on bureaucratic administration" based on information technology it occurs as a "normal" part of everyday life. Usually, surveillance results in power relations, in which the "watchers are privileged."[33]

---

[23] ibid.
[24] ibid.
[25] ibid.
[26] *S and Marper v UK* App nos. 30562/04 and 30566/04 (ECHR, 4 December 2008).
[27] ibid, [125].
[28] Ian Brown, 'Communications Data Retention in an Evolving Internet' (2010) International Journal of Law and Information Technology 19:2 95, 102-3.
[29] David Lyon, (n1), 13.
[30] IJClark, 'Digital privacy and digital citizens' (16 September 2016) <http://infoism.co.uk/2016/09/digital-citizens/> accessed 1 November 2016.
[31] David Lyon, (n1), 14; His definition has been cited by Wolfie Christl and Sarah Spiekermann, 'Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy'(2016) <http://www.privacylab.at/wp-content/uploads/2016/09/Christl-Networks__K_o.pdf> accessed 1 November 2016, p9; Alice E. Marwick, 'The Public Domain: Surveillance in Everyday Life' (2012) Surveillance & Society 9:4 378, 380; Ashlin Lee and Peta Cook, 'Seeing through the PRISM: the history of everyday surveillance' *The Conversation* (Melbourne, June 2013) <http://theconversation.com/seeing-through-the-prism-the-history-of-everyday-surveillance-15139> accessed 1 November 2016.
[32] Oxford Living Dictionaries <https://en.oxforddictionaries.com/definition/surveillance> accessed 16 November 2017.
[33] Wolfie Christl and Sarah Spiekermann, (n31).

Lyon does not determine what 'attention' means in the surveillance context, nor does he consider by whom or what 'focus' is attached to.[34] Without considering the purposes of said surveillance, this definition, it is contended, does not fully appreciate the significance of the retention of communications data as the definition begins with surveillance being focused on individuals. This would therefore disqualify data retention (or CCTV for example) from the ambit of Lyon's definition, even if it satisfied the other requirements of systematic and routine. As noted earlier, AG Saugmandsgaard Øe in *Tele2 and Watson* and various UK Lords during the passage of the Anti-terrorism, Crime and Security Bill[35] noted how data retention could affect substantial segments of the population. The Court of Justice of the European Union (CJEU) in the case C-293/12 (*Digital Rights Ireland*) noted how Directive 2006/24 (Data Retention Directive, DRD) covered all subscribers and registered users and therefore entailed an interference with the fundamental rights of *practically the entire European population* (author's emphasis).[36] The CJEU went further and elaborated that the DRD covered:

> …in a *generalised manner, all persons and all means of electronic communication* as well as all traffic data *without any differentiation*, *limitation or exception* being made in the light of the *objective of fighting against serious crime* (author's emphasis).[37]

Secondly, Lyon refers to surveillance as being systematic i.e. intentional, deliberate and does not happen randomly or spontaneously. Although data retention can be ordered, say in a retention notice, which is by definition deliberate, the effects of said notice cannot be said to be anything *but* spontaneous. Having one's data retained is entirely dependent upon the *telecommunications operator* they use. Section 1(5) of the Data Retention and Investigatory Powers Act 2014 (DRIPA 2014) noted that retention notices must not exceed 12 months. The DRD allowed data to be retained for between 6 to 24 months. The CJEU in *Digital Rights Ireland* critiqued this as permitting retention 'without any distinction being made between the categories of data…on the basis of their possible usefulness… or according to the persons concerned.'[38] DRIPA 2014 made no such distinction between categories of data to be retained, nor does the IPA 2016 and therefore would affect individuals solely based on the service they used. This would also affect those who may not use a service that is subject to a retention notice because the fact that they are the receiver of information subjects them to being passive subjects of retention.[39] This indicates the randomness as to the effects of data retention. The CJEU in *Tele2 and Watson* has now outlawed general and indiscriminate data retention.[40] The CJEU further qualified data retention by holding that the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted should be limited to what is strictly necessary.[41] However, the CJEU did permit retention on the basis which makes it possible to identify a public,[42] which could argued to be 'focussed.' But in the same vein, this identifiable public criterion is not based on individual suspicion,[43] and therefore it is submitted that this does not truly reflect the focussed nature of surveillance powers. The

[34] Paul Bernal, 'Data gathering, surveillance and human rights: recasting the debate,' (2016) Journal of Cyber Policy 1:2 243, 249.
[35] See section 5.1.
[36] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECR I-238, [56].
[37] ibid, [57].
[38] ibid, [63-64].
[39] Romania Constitutional Court DECISION no.12581 from 8 October 2009.
[40] Joined Cases C‑203/15 and C‑698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-970, [134].
[41] ibid, [108].
[42] ibid, [111].
[43] *Roman Zakharov*, (n16), [44-48], [260].

AG Saugmandsgaard Øe in *Tele2 and Watson* noted a disadvantage of data retention is 'the fact that the *vast majority of the data retained will relate to persons who will never be connected in any way with serious crime* (author's emphasis).'[44] Unless data retention, or more correctly, data preservation[45] is based and used upon reasonable suspicion[46] surveillance in this context can never truly be focussed.

Thirdly, Lyon's definition refers to surveillance as being routine. This would only be relevant insofar as data retention continuously or routinely affects the fundamental rights of those concerned, not to the fact that a retention notice, for example, need only be issued once a year and therefore, not on a day-to-day basis. Regarding attention, Lyon did not specify whether this meant man or machine attention, if it is the former, then again, data retention would be disqualified because no human attention is required for the actual retention of data. If, however, attention does not require human intervention, this still would not qualify data retention as surveillance because it is not focussed on individuals. Finally, Lyon's definition of surveillance is silent on information being stored, and only refers to day-to-day collection without elaborating from whose perspective, the watcher or the watched. It is therefore important to consider other ideas of surveillance as Lyon's definition may no longer adequate for some modern forms of surveillance, such as data retention.

Lyon himself, accepts that there are exceptions to his definition, giving the example of police general surveillance, in the form of a 'dragnet.'[47] Lyon suggests these exceptions are important as they add nuance to understanding the bigger picture.[48] Indeed, these types of surveillance are of vital importance in understanding it, but it will be argued that such measures of surveillance should not be regarded as 'exceptions.'

Moreover, Fuchs regards Lyon's surveillance studies as being ambivalent in character, in that he adopts both neutral and negative connotations of surveillance.[49] Fuchs defines neutral concepts of surveillance making one or more assumptions:

1. There are positive aspects of surveillance.
2. Surveillance has two faces, it is enabling and constraining.
3. Surveillance is a fundamental aspect of all societies.
4. Surveillance is necessary for organization.
5. Any kind of systematic information gathering is surveillance.[50]

This negative concept of surveillance is inherently linked to information gathering for the purposes of domination, violence, and coercion.[51] In an analogy to data retention, Lyon argues that just because a network of searchable databases appears to be able to track down minute details of personal life, does not mean it will do so, and if it does so, this does not mean it will have a negative impact on the individual.[52] This may be true as an individual may never know

[44] Opinion of Saugmandsgaard Øe, (n12), [252].
[45] Caspar Bowden, 'Digital Surveillance, Chapter Five Part I' (28 April 2013) <https://www.openrightsgroup.org/ourwork/reports/digital-surveillance/Chapter-five-part-i> accessed 2 January 2017.
[46] See Chapter 7.
[47] David Lyon, (n1), 15.
[48] ibid.
[49] Christian Fuchs, 'How can surveillance be defined?' (2011) Matrizes 5:1 109, 123.
[50] ibid, 111.
[51] ibid, 114.
[52] David Lyon, (n1), 10.

they are the subject of a database query, but this may nevertheless infringe fundamental rights, and so measurable negative impacts are only relevant to a certain degree. This however, constrains privacy to quantifiable harms resulting in fewer privacy problems being recognised.[53]

Lyon also maintains that surveillance is an ordinary part of everyday life even though it may sometimes take extraordinary turns.[54] This it is submitted, lies the danger of normalising surveillance, just because it happens very frequently, does not presuppose that this should be considered 'ordinary.'

(b) Rejecting the normalisation of surveillance

Wood and Webster elaborate on this point describing the UK's position as a bad example.[55] They argue that the normalisation of surveillance has important ethical and political consequences, which although inevitable for everyday life, have to be called into question.[56] They also note that the normalisation of surveillance in the UK has gone much further than elsewhere and because the UK is considered a 'model' to be aspired to by security professionals, the threat of the UK being a bad example to other European nation-states becomes very real. Support from this can come from the fact that it was the UK that played a major role in the EU adopting the DRD, and that subsequent EU Member states' national court's ruling that national implementation was unconstitutional. That is not to say, that the EU does not unilaterally act to increase surveillance capabilities.[57] Wood and Webster point out that the domestication of security and globalisation of surveillance would be 'limited if their results did not become increasingly 'normal' and part of the experience of everyday life.'[58] Continuing that:

> What would in the previous mode of ordering be regarded as temporary or even entirely unacceptable becomes unremarkable, mundane, normal and consequently may not even be challenged.[59]

Wood and Webster use the example of CCTV in the UK to demonstrate this. They highlight how remarkable it was by the distinct lack of non-academic opposition, and the evidence which questions the efficiency of CCTV.[60] Wood and Webster then question why was this so. They point to several reasons:

1. What CCTV represents, rather than what it does – showing 'something is being done' about the potential source of risk, a 'security theatre.'
2. The perception that CCTV is there [for the protection of] people.
3. Normalisation of CCTV through its footage and the birth of reality TV.

---

[53] Daniel Solove, *Understanding Privacy* (Harvard University Press 2009), 29-30.
[54] David Lyon, (n1), 9.
[55] David Murakami Wood and C. William R. Webster, 'Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain's Bad Example' (2009) Journal of Contemporary European Research 5:2 259.
[56] ibid, 259-260.
[57] ibid, 262.
[58] ibid.
[59] ibid, 262-263.
[60] ibid, 263.

4. Allowing viewers to give visual narratives to the incomprehensible i.e. placing meaning, even if erroneous.[61]

Wood and Webster explain that none of these arguments have anything to do with the technological properties of cameras or actual functioning of the systems *per se*, but how surveillance works at the level of emotion, symbolism and culture. The normalisation of surveillance will occur when these three domains are colonised,[62] for example, using customer data for a 'hilarious new marketing campaign.'[63] Sheridan adds that social conditioning and the normalising of the presence of surveillance devices has conditioned the wider population to ignore the lenses. CCTV is designed to be unobtrusive so that the gaze of the subjects passes over them, allowing for various overlapping lines of sight for whomever happens to be in the control booth.[64] Wood and Webster also noted that another reason is the computerisation of services, making it more citizen friendly and citizen-focussed. This dataveillance, 'the management and categorisation of data derived from surveillance' is seen to be working to provide what citizens want – the efficient and convenient delivery of public services and without it, put these services at risk. This functioning reinforces the normality of the collection, storage and sorting of large amounts of personal data, and the privileged or protected access or even 'ownership' of personal data by the state or, increasingly, its private partners or subcontractors.[65] Wood and Webster maintain this reduces social negotiations to 'no longer about what information one chooses to give but how that information is to be given (or taken).'[66] An example of this is the tracking MAC addresses when members of the public use the London Underground.[67]

This argument also rings true for data retention, as noted above, there is the flat-out denial that data retention is surveillance. There was also a letter written by the then Home Secretary, David Blunkett MP advocating that data retention 'is a private function that arises out of the commercial service that the communication service providers provide.'[68] This a clear misdirection which can shift the focus onto private companies[69] when they and the state require equal attention. The rhetoric of not having these laws would be 'putting lives at risk'[70] and the

[61] ibid, 263-264.
[62] ibid, 264.
[63] Bryan Clark, 'Spotify is using billboards to call users out on their questionable listening habits' (30 November 2016) <http://thenextweb.com/music/2016/11/30/spotify-is-using-billboards-to-call-users-out-on-their-questionable-listening-habits/> accessed 4 December 2016.
[64] Connor Sheridan, 'Foucault, Power and the Modern Panopticon' (2016) Senior Theses, Trinity College, Hartford, CT 2016. Trinity College Digital Repository <http://digitalrepository.trincoll.edu/theses/548> accessed 25 November 2016.
[65] David Murakami Wood and C. William R. Webster, (n55), 265.
[66] ibid.
[67] Gareth Corfield, 'TfL to track Tube users in stations by their MAC addresses' *The Register* (London, 17 November 2016) <http://www.theregister.co.uk/2016/11/17/tfl_to_track_tube_users_by_wifi_device_mac_address/> accessed 22 November 2016.
[68] Joint Committee on Human Rights, *Legislative Scrutiny: Draft Voluntary Code of Practice on Retention of Communications Data under Part 11 of the Anti-terrorism, Crime and Security Act 2001* (*sixteenth report*) (2002-03, HL 181, HC 1272) 19.
[69] Jim Dwyer, 'National Security Agency Said to Use Manhattan Tower as Listening Post' *The New York Times* (New York City, 17 November 2016) <http://www.nytimes.com/2016/11/18/nyregion/national-security-agency-said-to-use-manhattan-tower-as-listening-post.html?smid=tw-share&_r=0> accessed 20 November 2016.
[70] BBC, 'Theresa May says 'lives at risk' without data surveillance' *BBC News* (London, 15 January 2015) <http://www.bbc.co.uk/news/uk-politics-30816331> accessed 20 November 2016.

urgency for the DRD in light of the London 7/7 bombings[71] despite the then Prime Minister Tony Blair implying 'all the surveillance in the world' could not have prevented the attacks[72] highlights the tactics used to normalise data retention.

Wood and Webster continue to critique those that refer to the term 'surveillance society' as it is bland which although recognises the widespread usage of surveillance technologies but tells little how these technologies are felt, experienced or the different dimensions and deviations in surveillance practice.[73] Wood and Webster also point out that due to databases: 'in time, given the right (or wrong) circumstances we can all retrospectively become suspects - which *means that we are actually always already potential suspects* (author's emphasis).'[74] Wood and Webster finally conclude that changes to the normalisation need to come from the demand of citizens, to increase knowledge of surveillance and its consequences, to learn lessons from continental Europe so that where surveillance has become normal, it can be made strange and questionable again, and where it remains unusual to keep it the subject of active political debate. Nor should liberties be a matter of state manipulation at the constant shifting of goal posts in the name of security. The idea that living in a world of changing and flexible threats to security means that human rights are equally mutable and ephemeral needs to be resisted.[75]

In warning of the dangers of surveillance,[76] Richards points to the lack of understanding of privacy and why it matters as a reason of why we may not know why surveillance is bad and should be wary.[77] Haggerty notes that it is difficult for Westerners to envision and appreciate the dystopian potentials inherent in certain technologies.[78] To which Sheridan adds it is for more comforting to assume that 'If I have nothing to hide, I have nothing to fear' which of course is a mindset deliberately cultivated by the same institutions that gather the data in the first place.[79] In time, Sheridan continues, this 'lack of imagination on the possible, and even probable, logical extreme of mass surveillance and the modern panopticon could prove disastrous.'[80] This mindset, Sheridan adds, means that the general public are largely unaware when a new technology enters the game (such as artificial intelligence in CCTV)[81] and exploits them in ways they never thought possible, in which little can be done to prevent it because such abuses of power were never conceived of.[82] One way argued to combat normalisation of surveillance, is to restrict or prohibit indiscriminate surveillance technologies.[83]

---

[71] Chris Jones & Ben Hayes, 'The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy' (2013) <http://www.statewatch.org/news/2013/dec/secile-data-retention-directive-in-europe-a-case-study.pdf> accessed 20 November 2016, 8-9.
[72] Simon Davies, 'Unlawful, unworkable, unnecessary' *The Guardian* (London, 13 July 2005) <https://www.theguardian.com/world/2005/jul/13/humanrights.july7> accessed 20 November 2016.
[73] David Murakami Wood and C. William R. Webster, (n55), 265.
[74] ibid, 268.
[75] ibid, 270.
[76] Neil Richards, 'The Dangers of Surveillance' (2013) HARV. L. REV. 126 1934, 1935.
[77] ibid, 1934.
[78] Kevin D. Haggerty and Amber Gazso, 'Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats' (2005) The Canadian Journal of Sociology 30:2 169, 184.
[79] Connor Sheridan, (n64), 61.
[80] ibid, 62.
[81] Mahesh Sapharishi, 'The New Eyes of Surveillance: Artificial Intelligence and Humanizing Technology' *Wired* (San Francisco, California, August 2014) <https://www.wired.com/insights/2014/08/the-new-eyes-of-surveillance-artificial-intelligence-and-humanizing-technology/> accessed 18 November 2017.
[82] ibid.
[83] Danielle Keats Citron and David C. Gray, 'Addressing the Harm of Total Surveillance: a Reply to Professor Neil Richards' (2013) Harvard Law Review Forum 126 262.

Hintz and Dencik's supports Wood and Webster's view noting that despite the Snowden revelations and invalidation of the DRD, 'government policy in the immediate aftermath… was marked by the continuation and expansion of surveillance powers.'[84] This was made with reference to the DRIPA 2014 and the IPA 2016.[85] In the original draft Communications Data Bill (dCDB), this fell on telecommunications operators, which has since been replicated in the IPA 2016, essentially, different law, same provision and purpose, and therefore adding to its normalisation. This demonstrates a continuation of the dCDBill and an expansion of the Regulation of Investigatory Powers Act 2000 (RIPA 2000). As Wood and Webster noted, to challenge the normalisation of surveillance, it requires challenge from informed citizens etc, but Hintz and Dencik note this is limited to specific digital rights groups and does not resemble the protests seen in the US and Germany.[86] This was not helped by media bias as much reporting on the Snowden revelations were used to justify mass surveillance, leading to a notably muted[87] UK public response.[88] One member of a UK-based focus group said 'I think because so much of what we do is capable of being collected now, I think we've gone beyond that point *[of challenging the collection of data]* (author's emphasis).'[89] Shoshana Zuboff calls this 'psychic numbing' which 'inures people to the realities of being tracked, parsed, mined, and modified – or disposes them to rationalize the situation in resigned cynicism.'[90] Due to the lack of public challenge, media justification, strong role of security discourse and governmental composition:

> [H]ave hindered a more fundamental review of surveillance practices so far and have moved policy debate towards the expansion, rather than the restriction, of surveillance in the aftermath of Snowden.[91]

This normalisation of surveillance, does not just have implications for the UK. As Wood and Webster, and Hintz and Dencik highlight the UK being a 'model'[92] could influence other countries, particularly those with authoritarian regimes and poor human rights records.[93] Another aspect, not considered by Hintz and Dencik which could contribute to the normalisation of surveillance, is lack of will to hold those that carry out unlawful surveillance to account.[94]

---

[84] Arne Hintz and Lina Dencik, 'The politics of surveillance policy: UK regulatory dynamics after Snowden' (2016) Internet Policy Review 5:3 1, 5.
[85] See also Chapter 6 for the expansion of the definition of telecommunications operator.
[86] Arne Hintz and Lina Dencik, (n84), 8.
[87] John Naughton, 'Edward Snowden: public indifference is the real enemy in the NSA affair' *The Guardian* (London, 20 October 2013) <https://www.theguardian.com/world/2013/oct/20/public-indifference-nsa-snowden-affair> accessed 10 December 2016; Ewen MacAskill, ''Extreme surveillance' becomes UK law with barely a whimper' *The Guardian* (London, 19 November 2016) <https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper> accessed 11 December 2016.
[88] Arne Hintz and Lina Dencik, (n84), 9-10.
[89] ibid, 10.
[90] Shoshana Zuboff, 'Big other: surveillance capitalism and the prospects of an information civilization' (2015) Journal of Information Technology 30:1 75, 84.
[91] Arne Hintz and Lina Dencik, (n84), 11.
[92] ibid.
[93] Open Rights Group, 'THE INVESTIGATORY POWERS BILL'S IMPACT WILL REACH BEYOND THE UK' (2016) <https://www.openrightsgroup.org/press/releases/2016/ipb-will-reach-beyond-the-uk> accessed 21 November 2016.
[94] This is in reference to Phorm, which will be discussed in the next Chapter.

Another critique of normalising surveillance stems from Fuchs, who argues that if everything is surveillance, it becomes difficult to criticise repressive forms of it.[95] Though it could be argued all systematic collection of data is negative, because it interferes with fundamental rights, and criterion such as the justification for the collection, the use of data, consent and other factors that could be used determine whether this remains negative. As Fuchs notes, surveillance tries to bring about behavioural changes in which data that is processed can be 'so that potential or actual physical, ideological, or structural violence can be directed against humans in order to influence their behaviour.'[96]

(c) General Surveillance is Not the Exception

In continuing with defining surveillance, Lyon's own previous definition was 'any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered.'[97] Such a definition would have encapsulated data retention, however, his later definitions (see above) have been reaffirmed.[98]Lyon considers that general surveillance measures are the exception, this, however, is untrue. As Higgs noted, the collection of vast amounts of data is something that has occurred for hundreds of years. There are more recent examples, such as the invalidation of the DRD by the CJEU in *Digital Rights Ireland* which had faced constitutional challenges in various EU Member states. The CJEU's ruling in the case of C-362/14 (*Schrems*) declared that the Commission's US Safe Harbour Decision is invalid, because it authorised on a *generalised basis*, storage of all the personal data of all the persons whose data was transferred from the EU to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down for determining the limits of the access of the public authorities to the data and of its subsequent use (author's emphasis).[99] The ECtHR's Grand Chamber (GC) judgment in *Zakharov v Russia* ruled that Russia's surveillance measures, which amongst other things allowed 'interception of all telephone communications in the area where a criminal offence has been committed'[100] violated Article 8 of the ECHR.[101] Not long after *Zakharov* the ECtHR ruled on surveillance again in *Szabo and Vissy v Hungary* where it was ruled that the new technologies which enabled the Government to '*intercept masses of data* easily concerning even persons outside the original range of operation' without any safeguards violated Article 8.[102] The ECtHR in *Big Brother Watch* has also ruled that regime (brought to light by Snowden) for external surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA 2000) was incompatible with Articles 8 and 10.[103] There was also the CJEU's judgment in *Tele2 and Watson* ruled that blanket and indiscriminate data retention as unlawful. There is a cases pending in ECtHR on data retention,[104] and in the CJEU

[95] Christian Fuchs, (n49), 126.
[96] ibid, 128.
[97] David Lyon, *Surveillance society: monitoring everyday life* (Buckingham: Open University Press 2001), 2.
[98] David Lyon, 'Surveillance, power, and everyday life' in Chrisanthi Avgerou, Robin Mansell, Danny Quah, and Roger Silverstone (eds) *The Oxford Handbook of Information and Communication Technologies* (Oxford University Press 2009), 2.
[99] Case C‑362/14 *Schrems* [2015] ECR-I 650, [93], [107].
[100] *Roman Zakharov*, (n16), [265].
[101] ibid, [305].
[102] *Szabo and Vissy v Hungary* App no. 37138/14 (ECHR, 12 January 2016), [89].
[103] *Big Brother Watch v UK* App nos. 58170/13, 62322/14 and 24960/15 (ECHR, 13 September 2018).
[104] *Breyer v Germany* App no. 50001/12 Communicated on 21 March 2016.

on the new Safe Harbour termed Privacy Shield.[105] On 4 November 2015, then Home Secretary, Theresa May MP, admitted that s.94 of the Telecommunications Act 1984 (TA 84) had been used to allow security and intelligence agencies to gain access, in bulk, to communications data from communication service providers, both domestically and abroad.[106] Section 94 directions prior to 4 November 2015, and directions by the Foreign Secretary prior to October 2016 have been ruled unlawful by the Investigatory Powers Tribunal (IPT).[107] The Independent Reviewer of Terrorism Legislation, David Anderson, published his findings into the proven operational case for the use of bulk powers (such as bulk interception, bulk acquisition of communications data and compiling bulk personal datasets) by the UK's security and intelligence services.[108] The UK Government has implemented similar powers in the IPA 2016.[109] There are even allegations that six police forces in the UK have brought 'IMSI-catchers' that can both track the movements of mobile phone users within a given area, and intercept texts and calls.[110] UK police forces are also rolling out facial recognition camera's which are subject to legal challenges.[111] In addition to the tracking of MAC addresses mentioned earlier, not informing customers that e-receipts can be declined,[112] sharing patient data without consent,[113] Virtual Alabama in the US which combines three-dimensional satellite/aerial imagery of the state with geospatial analytics that reveal relationships, trends, and patterns in incoming data all add to the non-exceptional nature of general surveillance.[114] Such surveillance practices are not limited to the US or Europe.[115]

Despite Lyon maintaining his later definition of surveillance, he accepts that 'surveillance practices have been moving steadily from targeted scrutiny of ''populations'' and individuals to mass monitoring in search of what Oscar Gandy calls ''actionable intelligence.''[116] It is

[105] Julia Fioretti and Dustin Volz, 'Privacy group launches legal challenge against EU-U.S. data pact leftright 3/3leftright' *Reuters* (London, 27 October 2016) <http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN12Q2JK> accessed 2 November 2016.
[106] HC Deb 4 November 2015, vol 601, col 971.
[107] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2016] UKIPTrib 15_110-CH, [111]; *Privacy International v v Secretary of State for Foreign and Commonwealth Affairs and Others* [2018] UKIPTrib IPT_15_110_CH, [113].
[108] David Anderson, 'Report of the Bulk Powers Review' (August 2016) <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf> accessed 2 November 2016.
[109] Part 6.
[110] Alon Aviram, 'Revealed: Bristol's police and mass mobile phone surveillance' (October 2016) <https://thebristolcable.org/2016/10/imsi/> accessed 22 October 2016.
[111] Lizzie Dearden, 'Police accused of deploying facial recognition 'by stealth' in London' *The Independent* (London, 27 July 2018) <https://www.independent.co.uk/news/uk/crime/facial-recognition-uk-police-london-trial-data-human-rights-legal-action-met-a8466876.html> accessed 28 July 2018.
[112] Jon Baines, 'Don't be so soft' (22 November 2016) <https://informationrightsandwrongs.com/2016/11/22/dont-be-so-soft/> accessed 23 November 2016.
[113] Natasha Lomas, (22 November 2016) <https://techcrunch.com/2016/11/21/deepmind-health-inks-new-deal-with-uks-nhs-to-deploy-streams-app-in-early-2017/> accessed 23 November 2016.
[114] Danielle Keats Citron and David C. Gray, (n82), 263.
[115] Matt Payton, 'Japan's top court has approved blanket surveillance of the country's Muslims' *The Independent* (London, 29 June 2016) <http://www.independent.co.uk/news/world/asia/muslims-japan-government-surveillance-top-court-green-lit-islamaphobia-a7109761.html> accessed 2 November 2016; Terence Lee, 'Singapore an advanced surveillance state, but citizens don't mind' *TechCrunch* (Bay Area, 26 November 2013) <https://www.techinasia.com/singapore-advanced-surveillance-state-citizens-mind> accessed 2 November 2016.
[116] David Lyon, 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique' (2014) Big Data & Society July–December 1:2 1–13, 2.

unclear what distinction Lyon is asserting to make between targeted scrutiny[117] of populations and mass monitoring as both can mean the same thing. The similarities lie in what is defined as "populations" (which Lyon does not define) as both European Courts have noted, certain surveillance measures can potentially affect all (of the population) within a state's jurisdiction and can therefore amount to mass monitoring. General measures of surveillance can no longer be, if they ever were, considered exceptions but the norm.

Lyon also maintains that 'surveillance data are not gathered about everyone in the same way, or with the same intensity.'[118] This, however, depends on the mode of surveillance as powers of general data retention and bulk powers tend not to make distinction between individuals concerned or data to be obtained.

Heather Brooke correctly noted that with bulk collection powers, 'the potential exists for *anyone to be watched at any time* (author's emphasis)' and the 'point of Jeremy Bentham's Panopticon wasn't that everyone was actually watched at all times, *it was that they could all potentially be watched* (author's emphasis).'[119] Although this Chapter will propose an argument that extends beyond AG Cruz Villalón's Opinion in *Digital Rights Ireland*, it does highlight similarities between data retention and the Panopticon. A-G Cruz Villalón noted that:

> The *collection of such data establishes the conditions for surveillance* which, although carried out only retrospectively when the data are used, none the less *constitutes a permanent threat throughout the data retention period to the right of citizens of the Union* to confidentiality in their private lives. The *vague feeling of surveillance* created raises very acutely the question of the data retention period (author's emphasis).[120]

This reasoning opened up the idea of data retention creating the circumstances that enabled EU citizens to be watched anytime their data was accessed. This facilitates a discussion on Bentham's Panopticon, later works in its relationship with surveillance and its relevance to untargeted measures of surveillance.

5.4 Bentham's Panopticon

The idea of the Panopticon was first coined by Jeremy Bentham,[121] who believed the Panopticon, or Inspection House[122] would be a 'new mode of obtaining power of mind over mind' in unknown quantities and degrees to those who choose to have it.[123] Bentham articulated that *the more constantly the persons to be inspected are under the eyes of the persons who should inspect them*, the more perfectly will the purpose of the establishment have been attained (author's emphasis). In addition to this, Bentham highlighted that ideal perfection

---

[117] This in itself can be problematic as it assumes that everyone within that "population" is of interest. If there are individual's within a population that are of interest, yet the entire population are under surveillance, it is difficult to suggest the measure is targeted, just as noted in *Zakharov*.
[118] David Lyon, (n1), 18.
[119] Heather Brooke, 'Mass surveillance: my part in the reform of GCHQ and UK intelligence gathering' *The Guardian* (London, 14 July 2015) <https://www.theguardian.com/commentisfree/2015/jul/14/mass-suveillance-reform-gchq-uk-intelligence-gathering-rusi-report> accessed 2 November 2016.
[120] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] ECR I-845, Opinion of Cruz Villalón, [72].
[121] Jeremy Bentham, The Works of Jeremy Bentham, vol. 4 [1843] (September 2011) <http://lf-oll.s3.amazonaws.com/titles/1925/Bentham_0872-04_EBk_v6.0.pdf> accessed 3 November 2016.
[122] ibid, p65.
[123] ibid, p67.

would require continuous inspection, but knew this to be impossible.[124] It is as this point when Bentham's first letter highlights one of the fundamentals of his Panopticon, namely that the inspector should *conceive* themselves as all seeing.[125]

The Panopticon consisted of a circular building, with prisoners occupying the circumference. Prisoners would be secluded from one another, separated by cells. The apartment of the inspector would occupy the centre, which would be separated from the circumference by vacant space.[126] The inspector would not be able to see all inmates simultaneously, they would have to adjust their positions accordingly.[127]

This demonstrates that although inspection cannot occur to everyone at all times, it creates the circumstances in which *anyone* could be watched highlighting the link between the Panopticon and data retention as noted by Heather Brookes and AG Cruz Villalón's where anyone's data could be 'viewed.' To argue that data retention is a form of surveillance likened to a Panopticon, it is important to consider Michel Foucault's vision of power, discipline, and the Panopticon.

5.5 Foucault's Discipline and Punish

Foucault is arguably the most influential thinker for the elaboration of negative surveillance concepts.[128] Fuchs maintains that Foucault regarded surveillance as a form of disciplinary power, which are regarded as 'general formulas of domination.'[129] This is derived from what Foucault considers disciplines of the body which included an:

> …uninterrupted, constant coercion, super- vising the processes of the activity rather than its result and it is exercised according to a codification that partitions as closely as possible time, space, movement.[130]

Domination, Foucault observed, encloses humans to various institutions in order to control behaviour, partition and rank[131] and to normalise punishment, hierarchies, homogenise, differentiate, and exclude.[132] Foucault argued that for successful disciplinary power, it required hierarchical observation, the normalising judgement, and the examination.[133] Foucault continued that the exercise of discipline required a mechanism that coerced by means of observation 'an apparatus in which the techniques *that make it possible to see* induce effects of power (author's emphasis)'[134] For example, the retention of communications data, makes it possible for data to be accessed, therefore making it possible to 'see' into the lives of those whose data has been retained. Big Data, of course, making this much easier. Information asymmetries[135] can provide and facilitate power, and that the collection and use of metadata

[124] ibid.
[125] ibid.
[126] ibid, p71.
[127] ibid.
[128] Christian Fuchs, (n49), 115.
[129] ibid; Michel Foucault, (n2), 137.
[130] ibid.
[131] ibid, 141.
[132] ibid, 183.
[133] ibid, 170.
[134] ibid, 170-171.
[135] Bart W. Schermer, 'Surveillance and Privacy in the Ubiquitous Network Society' (2009) 1:4 <http://amsterdamlawforum.org/article/view/95/169> accessed 22 November 2017.

can significantly impact the relationships between governments and their citizens.[136]

Another form of domination, referred to as 'dehumanisation' by Solove is based upon the Kafka metaphor in which databases foster a state of powerlessness and vulnerability created by people's lack of any meaningful form of participation in the collection and use of their personal information.[137]

In the specific context of data retention, Roberts argued that domination is a condition that can exist *in the absence of such awareness* of it.[138] Roberts maintains that acquisition of data can allow inferences to be drawn about individuals' in which counterstrategies can be devised to manipulate and nudge individuals' to make particular choices.[139] Such manipulation Roberts contends, depends on the subject being unaware that they have suffered the loss of privacy and that information gained is used to ensure decisions are made based on the manipulators' preferences. This point is important *because awareness leaves open the possibility of resistance*.[140] Such an inability to resist would nullify Article 8.[141] The interference posed by data retention cannot solely be based on the nature of the data but also whom has access,[142] which are many, and thus a concern.[143] Basing his premise on Pettit's idea of domination (arbitrarily interfering with choices)[144] Roberts noted that if there isn't a nexus between the extent and exercise of power, it cannot be said to be a necessary means of meeting a stated objective.[145] It instead provides for those who:

> [P]ossess it with the capacity to interfere on an arbitrary basis – the power to interfere in ways that do not track the interests of who might be on the receiving end of it. It is the acquisition of such power that establishes the dominating relationship. *It does not matter whether or not the agent or agency that has acquired it is inclined to use it. The mere fact that it has been acquired is contrary to the interests of the subject of the loss*. It places him in a position of dependency vis-à-vis those who possess the power – his ability to choose freely is dependent on the continuing good will or benevolence of the agent or agency (author's emphasis).[146]

Roberts concluded that retention notices under DRIPA 2014 and would now be IPA 2016 would confer a dominating power against which individuals ought to be protected against by the right to privacy.[147]

---

[136] Bryce Clayton Newell, 'The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe' (2014) A Journal of Law and Policy for the Information Society 10:2 481, 482.
[137] Daniel J. Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) Stan. L. Rev. 53 1393, 1424. Franz Kafka's novel, *The Tria* tells the story of Joseph K whom is arrested and prosecuted by a remote, inaccessible Court, in which the nature of his crimes is never revealed to Joseph K despite his best efforts to uncover this (whom is subsequently killed) or to the reader.
[138] Andrew Roberts, 'Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications' (2015) 78:3 MLR 522, 544.
[139] ibid, 545.
[140] ibid.
[141] *Klass v Germany* App no. 5029/71 (ECHR, 6 September 1978), [36].
[142] Andrew Roberts, (n138), 545.
[143] Joseph Cox, 'Even the Food Standards Agency Could Access UK Surveillance Data Under New Bill' *Motherboard* (Montreal, 26 November 2015) <https://motherboard.vice.com/en_us/article/ezpddn/even-the-food-standards-agency-could-access-uk-surveillance-data-under-new-bill> accessed 27 November 2017.
[144] Philip Pettit, *Republicanism* (Oxford: OUP, 1997) 52.
[145] Andrew Roberts, (n138), 546.
[146] ibid.
[147] ibid, 548.

Surveillance for Foucault, secretly prepares a 'new knowledge of man' with the observer seeing 'without being seen.'[148] Foucault maintained that an almost ideal model for observation were these observatories i.e. the military camp which is 'the diagram of a power that acts by means of *general visibility*' the 'spatial 'nesting' of *hierarchized surveillance* (author's emphasis).'[149] Foucault believed that the 'perfect disciplinary apparatus would make it possible for a single gaze to see everything constantly' a 'perfect eye *that nothing would escape* and a centre towards which all gazes would be turned (author's emphasis).'[150] Analogies with data retention can be drawn in this regard, as the purpose of retention is to ensure that communications data does not escape. Although it is true that access to this data can be obtained by various public authorities, it is suggested that this 'centre' to which Foucault speaks of, could be regarded as the state.[151] Foucault referred to Ledoux when building the Arc-et-Senans,[152] all the buildings were to be arranged in a circle, opening on the inside, at the centre of which a high construction was to house the administrative functions of management. Foucault believed this allowed all activities to be recorded, perceived and judged.[153] Similar to data retention (recorded), which allows the possibility of access to data (perceived) which in turn allows a public authority to judge and act upon.

For Foucault, hierarchized surveillance of the disciplines is not possessed as a thing, or transferred as a property; but *functions like a piece of machinery*. This enables, Foucault argues 'the disciplinary power to be both absolutely indiscreet, since it is everywhere and always alert' and 'absolutely 'discreet, for it functions permanently and largely in silence.'[154] This, it is submitted, draws an analogy with data retention in that any number of individual's data can be retained without them ever knowing. In relation to normalising judgement, Foucault described at the heart of all disciplinary systems functions a small penal mechanism, referring to unwritten laws of punishment.[155]

This punishment (confusion, coldness, indifference etc)[156] could be associated with what is known as the chilling effect.[157] Under pervasive surveillance, individuals are inclined to make choices that conform to mainstream expectations.'[158] This would correlate with AG Cruz Villalón notion of data retention creating a vague sense of surveillance. In addition to, this idea of a chilling is important as Solove has argued that when performing a balancing test, the social benefits of privacy should be principally considered.[159]

In regards to examination, Foucault noted 'that examination introduced a whole mechanism

[148] Michel Foucault, (n2), 171.
[149] ibid, 171-172.
[150] ibid, 173.
[151] ibid, 169-170.
[152] World Heritage Convention, 'From the Great Saltworks of Salins-les-Bains to the Royal Saltworks of Arc-et-Senans, the Production of Open-pan Salt' <http://whc.unesco.org/en/list/203> accessed 21 November 2017.
[153] Michel Foucault, (n2), 173-174.
[154] ibid, 177.
[155] ibid, 177.
[156] ibid, 178.
[157] See Chapter 4.
[158] Lilian Mitrou, 'The impact of communications data retention on fundamental rights and democracy – the case of the EU Data Retention Directive in Kevin D. Haggerty and Minas Samatas (ed) *Surveillance and Democracy* (Routledge and Cavendish 2010), 138; Elizabeth Stoycheff, 'Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring' (2016) Journalism & Mass Communication Quarterly 93:2 296.
[159] Daniel Solove, (n53), 89.

that linked to a certain type of the *formation of knowledge* a certain form of the exercise of power (author's emphasis).'[160] Thus, acquiring knowledge through examination demonstrates an exercise of power. In addition, Foucault noted that:

> Disciplinary power…is *exercised through its invisibility*; at the same time it imposes on those whom it subjects a *principle of compulsory visibility*. In discipline, it is the *subjects who have to be seen*. *Their visibility assures the hold of the power that is exercised over them*. It is the fact of being constantly seen, of *being able always to be seen* (author's emphasis).[161]

This, Foucault maintains, objectifies subjects of examination.[162] A similar analogy can be drawn between the secretive nature of data retention and the fact that individual's data is subject to state actions.

Further to this examination, Foucault notes that we are entering the age of the infinite examination (always seen) and of compulsory objectification.[163] Importantly, Foucault highlighted that examination introduces individuality into the *field of documentation* 'places individuals in a field of *surveillance also situates them in a network of writing; it engages them in a whole mass of documents that capture and fix them* (author's emphasis).'[164] These procedures of examination were accompanied at the same time by a system of intense registration and of documentary accumulation. A *'power of writing,'* Foucault contended was constituted as an essential part in the mechanisms of discipline.[165]

This keeping of records, Foucault contends, formed an integral part of the process in which those were subjected to the disciplinary regime.[166] Foucault noted that fundamental conditions of a good discipline must include procedures of writing that made it possible to integrate individual data into cumulative systems in such a way that they were not lost to enable individuals to be located in the general register in which each datum of the individual examination might affect overall calculations.[167] Foucault further added, thanks to the apparatus of writing it allowed the subjection of individuals 'under the gaze of a permanent corpus of knowledge' and 'constitution of a comparative system that made possible the measurement of overall phenomena…in a given 'population.'[168]

For Foucault, discipline is about the individualisation of subjects in a descending fashion where power becomes more anonymous and functional.[169] Foucault notes with examples of children being more individualised than the adult, the patient more than the healthy, the mentally ill and delinquent than the mentally stable and non-delinquent.[170] This notion of individualisation can also be turned on the healthy, the mentally stable, the law abiding.[171] Foucault is highlighting that surveillance need not be limited to those who are of interest, but to those who *might* be of

---

[160] Michel Foucault, (n2), 187.
[161] ibid.
[162] ibid.
[163] ibid, 189.
[164] Similar to 'social sorting' described in Chapter 4.
[165] Michel Foucault, (n2), 189.
[166] ibid, 190.
[167] ibid.
[168] ibid.
[169] ibid, 192.
[170] ibid.
[171] ibid.

interest, given the right information is obtained. This strikes a similarity to the DRD, as Judge Pinto de Albuquerque in his concurring opinion in *Szabo* and *Vissy*, noted that it created compulsory, *suspicion-less*, and untargeted data retention obligations.[172]

(a) Foucault and the Panopticon

Foucault believed that the Panopticon[173] was surveillance that is based on *a system of permanent registration*[174]in which all events are recorded.[175] For Foucault, the Panoptic 'mechanism arranges spatial unities that *make it possible to see constantly* and to recognize immediately (author's emphasis).'[176] Individuals in Panoptic mechanisms, Foucault believed were the object of information and never a subject in communication.[177] A major effect of the Panopticon is to induce 'a state of conscious and permanent visibility' ensuring the automatic functioning of power.[178] Foucault continues that this arranges 'things that the *surveillance is permanent in its effects*, *even if it is discontinuous in its action* (author's emphasis).'[179] Foucault further adds that 'the perfection of power should tend to *render its actual exercise unnecessary* (author's emphasis).'[180] Foucault articulated that it would be too much and too little for individuals to be constantly observed, too little as what matters is that individuals know they are being observed, and too much he has *no need of being so*.[181] Referring to Bentham, Foucault noted that power should be visible and unverifiable, visible in that individuals know that they are spied upon, and importantly unverifiable because individuals must *never know* whether they are being looked at in any given moment, but must be sure that they may always be so.[182] Regarding data retention, for example, the DRD enacted and implemented by Member States could be argued as satisfying the requirement of visibility, this may also be more apparent due to greater awareness since the Snowden revelations. Unverifiable as the CJEU noted that it interfered with the fundamental rights of *practically the entire European population*[183] in a generalised manner.[184] The unverifiable notion accords with a corresponding ECHR safeguard in that under certain circumstances an individual can claim to be a victim of a violation of the Convention by the *mere existence* of secret measures or laws permitting such measures *without having to allege they were actually applied to them*.[185]

Foucault maintained that due to the mechanisms of observation, the Panopticon gains in efficiency and in the ability to penetrate into behaviour in which knowledge follows the advances of power, that can lead to discovering new objects of knowledge over all the surfaces on which power is exercised.[186] Similar to data retention which allows knowledge to be obtained from communications data which can then subsequently be matched up with other communications data, this can be amplified with Big Data.[187] In other words,

[172] *Szabo and Vissy*, (n102), [15].
[173] Michel Foucault, (n2), 200.
[174] ibid, 196.
[175] ibid, 197.
[176] ibid, 200.
[177] ibid.
[178] ibid, 201.
[179] ibid.
[180] ibid.
[181] ibid.
[182] ibid.
[183] *Digital Rights Ireland and Seitlinger and Others*, (n36).
[184] ibid, [57].
[185] *Klass*, (n139), [34]; *Roman Zakharov*, (n16), [171].
[186] Michel Foucault, (n2), 204.
[187] See generally Chapter 4.

knowledge/information is power,[188] and data is knowledge, whosoever has control over data, exercises power. Foucault regards the Panopticon as the 'perfect exercise of power'[189] because it can reduce the number who exercise power whilst increasing those who are subject to it.[190] In addition to this, Foucault adds it allows the intervention at any moment and because the constant pressure acts even before the offences, mistakes or crimes have been committed.[191] The strength of this, is that 'it never intervenes' and is 'exercised spontaneously and without noise.'[192] An analogy between Foucault's idea and data retention can be drawn, as access to communications data is made possible at any moment. This also contrasts with Lyon's definition of surveillance only being spontaneous as an exception.

Foucault regards surveillance as permanent, exhaustive and omnipresent 'capable of making all visible, as long as it could itself remain invisible.'[193] Foucault also noted that the ideal point of penalties would be 'an indefinite discipline' an 'interrogation without end' a 'judgement that would at the same time be the constitution of a file that was never closed.'[194] This is similar to the cyclical nature of data retention.[195]

Foucault argues that the drawing up of tables was one of the great problems of disciplinary power in the 18th century[196] Fuchs notes that the modern equivalent for tables are:

> …digital databases that store huge amounts of data that can be automatically collected, assessed, manipulated, and remixed, are available in real time, are distributed at high speed all over the world, are easy and cheap to collect and distribute, and can be duplicated without destruction of the original data. The computer database enables an extension and intensification of surveillance based on tables.[197]

Fuchs continues that computers and computer networks used for surveillance constitute what Foucault described as one of the 'innovations of disciplinary writing.'[198] It is this connection power/knowledge, Fuchs acknowledges, that Foucault stresses as constitutive for surveillance takes on the form of power/digital data in the information age.[199]

5.6 The Contemporary Panopticon

When Foucault reenergised his interpretation of Bentham's Panopticon, he did not have in mind the computerisation of surveillance, and this is where it is important to consider as Fuchs suggests, the Panopticon in the information age.

(a) Gordon and the Electronic Panopticon

[188] Geoffrey Lightfoot and Tomasz Piotr Wisniewski, 'Information asymmetry and power in a surveillance society' (2014) Information and Organization 24 214, 228.
[189] Michel Foucault, (n2), 206.
[190] ibid.
[191] ibid.
[192] ibid.
[193] ibid, 214.
[194] ibid, 227.
[195] See Chapter 7.
[196] Michel Foucault, (n2), 148.
[197] Christian Fuchs, (n49), 116.
[198] Michel Foucault, (n2), 190.
[199] Christian Fuchs, (n49), 116-117.

Diana Gordon was one of the first to consider the electronic Panopticon in terms of the National Criminal Records System in the United States.[200] Gordon highlighted that one of the most rapidly expanding, but least noticed state activities were the 'collection, combination, and dissemination of computerized criminal justice records.'[201] Gordon likened national computerised systems as a 'panoptic schema' with the record the surrogate as the inmate and law enforcement as the warden, which knows no bounds as the warden becomes the boss, landlord and banker, enclosing one in the electronic Panopticon.[202] Gordon highlighted that 'as the number and variety of records grows, along with the amount and kind of data contained in them, judgments about what persons and behaviours are appropriate subjects for data surveillance become less and less discriminating.'[203] Similarly with communications data retention, data retention is purely limited to which telecommunications operators a retention notice is issued upon and therefore more and more indiscriminate.

Gordon argues that with such systems '[t]he analogy of the 'panoptic schema,' which oppresses its subjects with the potential for surveillance as well as its actuality'[204] is relevant in this regard. Gordon continues that the managers of the modern Panopticon have at least the option of using every bit of available information.[205]

(b) Other forms of the Contemporary Panopticon

Shoshana Zuboff builds on Bentham's and Foucault's Panopticon, the 'Information Panopticon' and applies it to the work environment.[206] Unlike Bentham's envision, Zuboff's Information Panopticon did not rely upon physical structures and human supervision,[207] but instead, a computer that kept track of workers' every move and recorded it.[208] Sheridan notes that the workers in Zuboff's literature were far more likely to take more care in their work to ensure complications did not arise, and if they did, made sure that they could not be held liable. On a wider social level, this would entail that the public are more likely to look inward and engage in self-surveillance, monitoring both what they do and say to be more in line with social norms and not draw the attention of the system,[209] the chilling effect. Poster argued that:

> Today's 'circuits of communication' and the *databases* they generate constitute a Superpanopticon, *a system of surveillance without walls, windows, towers or guards* (author's emphasis).[210]

And so what we see here is how Betham's Panopticon has evolved[211] to encapsulate the information era, in particular, the recording, or retention of data.

---

[200] Diana R. Gordon, 'The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System' (1987) Politics & Society December 15:4 483.
[201] ibid, 483.
[202] ibid, 487.
[203] ibid, 496.
[204] ibid, 504.
[205] ibid.
[206] Shoshana Zuboff, *In the age of the smart machine: the future of work and power* (New York: Basic Books 1988).
[207] ibid, 322.
[208] ibid, 331.
[209] Connor Sheridan, (n64), 52-53.
[210] Mark Poster, *The mode of information* (Cambridge: Polity 1990), 93.
[211] Connor Sheridan, (n64), 5.

(c) David Lyon – from Big Brother to the Electronic Panopticon

For balance, a critique of the electronic Panoptic is considered by Lyon. Lyon in the mid-nineties considered how far the Panopticon provided a useful model for understanding electronic surveillance.[212] In discussing Orwell's *1984* Lyon remarks that '[t]he challenge of electronic surveillance is missed if it is reduced to a concern merely with privacy.' This is true given the analysis in Chapter 4. Lyon refers to the idea of Bentham's Panopticon as being significant because it gave the impression of an all-seeing power.[213]

But in his critique, Lyon refers to the Panopticon as only a powerful metaphor for understanding electronic surveillance.[214] Lyon notes that beyond the metaphor is the model, which Lyon refers to as the 'normalising of discipline, the exaggerated visibility of the subject, the unverifiability of observation, the subject as bearer of surveillance, the quest for factual certainty' and asks to what extent are they present in each context.[215]

Lyon cites Giddens and agrees that in different institutions, there is a difference in timescale when any individual is subjected to the Panopticon, giving the example that inmates are incarcerated all the time whereas schools etc, only part of the day is subjected to this. Lyon quite rightly maintains that one may now, due to advances in technology take it home with him as a consumer, creating the possibility of being subjected to the Panopticon. Lyon, however, believes that it was 'still not clear that this in itself augurs a general societal panopticism.'[216] Lyon makes this assertion, without actually assessing ways in which the Panopticon could affect those at home with new technologies such as Amazon Alexa, Apple's Siri, or for instance, the way in which s.94 of the Telecommunications Act 1984 (and the Digital Telephony Act) was utilised to obtain vast amounts of communications data. Of course, he could not have known because it was made public 19 years later, but this clearly satisfies the 'unverifiability of observation' Lyon spoke of. This highlights the possible continuous nature where one could be subjected to surveillance in for example, the workplace[217] *and* at home when using electronic devices in both instances particularly using work devices at home.[218] The use of s.8 of the RIPA 2000 for bulk interception, the DRD, the revelations of Snowden, and the IPA 2016 only serve to amplify this, and therefore the idea of 'the exaggerated visibility of the subject' weakens because it demonstrates just how unknowingly exposed to surveillance we have become. On 16 November 2016, the *Intercept* published an article detailing the extent of the National Security Agency's (NSA) surveillance practices.[219] This details that not only does the NSA gather as much intel on citizens, but under the BLARNEY program this allowed them to:

> [M]onitor communications related to multiple countries, companies, and international organizations. Among the approved targets were the International Monetary Fund, the

[212] David Lyon, 'From Big Brother to Electronic Panopticon' in David Lyon (ed) *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis: University of Minnesota Press, 1994) 57-80.
[213] ibid.
[214] ibid.
[215] ibid.
[216] ibid.
[217] *Copland v UK* App no. 62617/00 (ECHR, 3 April 2007).
[218] Chris Smith, 'iOS 9.3 will tell you if your employer is tracking your iPhone' (2 March 2016) <http://bgr.com/2016/03/02/work-iphone-privacy-ios-9-3/> accessed 21 November 2017.
[219] Ryan Gallagher and Henrik Moltke, 'TITANPOINTE The NSA's Spy Hub in New York, Hidden in Plain Sight' *The Intercept* (16 November 2016) <https://theintercept.com/2016/11/16/the-nsas-spy-hub-in-new-york-hidden-in-plain-sight/> accessed 17 November 2016.

> World Bank, the Bank of Japan, the European Union, the United Nations, and at least 38 different countries, including U.S. allies such as Italy, Japan, Brazil, France, Germany, Greece, Mexico, and Cyprus.[220]

Lyon then considers the links made between capitalism and the Panopticon. Lyon was of the opinion that consumers are seduced into conformity rather than coerced into compliance for fear of Big Brother.[221] It is true that products and services can be utilised to get consumers hooked,[222] but in the same vein, most people, even those that are studying areas related to surveillance and privacy are unlikely to read terms of services or privacy policies, and if they do, spend little time reading and therefore focussing what they want from a service, rather than privacy or data sharing concerns.[223] Obar and Oeldorf-Hirsch in a study demonstrated that 98% of participants agreed to corporations taking their child away in payment for use of their services.[224] Nehf uses the Hansel and Gretel metaphor in which we are:

> We are happily eating all the cookies, candy, and gingerbread, enjoying what we think are the benefits of sharing personal bytes of data in the information society. As we do so, we may be fattening ourselves for someone else's feast, unaware of the fate that may await us.[225]

Privacy trade-offs are also argued to be fallacious.[226] Moreover, Lyon made no mention of the 'Crypto Wars' in which governments 'fought to control the use of encryption, while privacy advocates insisted its use was essential — not just for individual freedom, but also to protect the commercial development of the nascent internet.'[227] This of course, demonstrated the *resistance* to Panoptic coercion. To a lesser degree this is also true when the issue becomes that of cookies, trackers and consent, many websites dump cookies on devices which can track user's online activity without consent,[228] or even coerce users into usage of services, accepting terms defined by said companies.[229] Even after Lyon's piece, this trend did not disappear as

---

[220] ibid.
[221] David Lyon, (n212).
[222] Nir Eyal, *Hooked: A Guide to Building Habit-Forming Products* (CreateSpace Independent Publishing Platform 2013).
[223] Jonathan A. Obar and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (24 August 2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465> accessed 9 December 2016.
[224] ibid, p25.
[225] James, P. Nehf, 'Recognising the Societal Value in Information Privacy' (2003) Wash. L. Rev. 78 1, 5.
[226] Joseph Turow, Michael Hennessy and Nora Draper, 'The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening them up to Exploitation' (June 2015) <https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_2.pdf> accessed 4 October 2017; Mark Andrejevic, 'The Big Data Divide' (2014) International Journal of Communication 8 1673, 1682-1686.
[227] Steve Ranger, 'The undercover war on your internet secrets: How online surveillance cracked our trust in the web' *TechRepublic* (Louisville, Kentucky, 12 June 2016) <https://web.archive.org/web/20160612190952/http://www.techrepublic.com/article/the-undercover-war-on-your-internet-secrets-how-online-surveillance-cracked-our-trust-in-the-web/> accessed 17 November 2016.
[228] European Commission, 'Cookies' <http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm> accessed 17 November 2016. Not all websites adhere to the model given by the European Commission.
[229] Christian Fuchs, 'New Media, Web 2.0 and Surveillance' (2011) Sociology Compass 5:2 134, 143; For other ways in which services elicit control see Glyn Moody, 'Google is threatening to throw me off Google+, but won't tell me why' *Ars Technica* (19 December 2016) <http://arstechnica.co.uk/information-technology/2016/12/google-is-threatening-to-throw-me-off-its-g-service-but-wont-tell-me-why/> accessed 21 December 2016; Sarah Jeong, 'Terror Scanning Database For Social Media Raises More Questions than Answers' *Motherboard* (Montreal, 9 December 2016) <https://motherboard.vice.com/read/social-media-terror-scanning-database> accessed 21 December 2016.

Marx identifies other forms of social control involving the requesting volunteers based on appeals to good citizenship or patriotism; using disingenuous communication (e.g. In entering here you have agreed to be searched); the trading of personal information for rewards and convenience; and utilising hidden or low visibility information collection techniques.[230] Furthermore, this intensifies with Big Data, where Rhoen notes that it is shifting power away from data subjects and consumers to the data controllers, allowing them to influence consumer behaviour or decision making.[231] Rhoen considers whether paid for or not, usage of services in exchange for the collection and use of personal data (for profit) amounts to 'privacy contracts.'[232] Rhoen continues that if data controllers become too powerful, the validity of consumers' and data subjects' consent or autonomy when entering into privacy contracts can be questioned.[233] Rhoen refers to Barnett and Duval who define power 'as the production, in and through social relations, of *effects that shape the capacities of actors to determine their circumstances and fate* (author's emphasis).'[234] Rhoen continues that data controllers use their existing structural power (lack of consumer bargaining power) over data subjects in the contracting phase to increase their institutional power after the contract is concluded (the data controller obtaining a method of exerting power over the consumer i.e. personal advertising).[235] Such unaccountable[236] power structures may have influenced the 2016 US Presidential Elections and the EU Referendum by influencing individuals to recruit them to an idea.[237]

The Panopticon may be used to control behaviour through fear, but that is not the only way in which the internalisation of control can occur, this could also be through guilt, embarrassment, shame, irritation[238] or even rewards.[239] Sheridan argues further that:

> [T]he most important thing to come out of Snowden's revelations was the return of panoptic power to the Foucaultian model.[240]

The Panopticon may not be the perfect idea of what constitutes surveillance, but it has helped shape understandings of surveillance in the past, present[241] and has implications for the future. Even if one were to agree that the Panopticon is just a powerful metaphor, Solove notes that:

> Metaphors function not to render a precise descriptive representation of the problem; rather, they capture our concerns over privacy in a way that is palpable, potent, and

[230] Gary Marx, 'Soft surveillance: the growth of mandatory volunteerism in collecting personal information – "Hey buddy can you spare a DNA"' in Torin Monahan (ed), *Surveillance and Security: Technological Politics and Power in Everyday Life*, (London: Routledge 2007).
[231] Michael Rhoen, 'Beyond consent: improving data protection through consumer protection law' (2016) Internet Policy Review 5:1 1.
[232] ibid, 2.
[233] ibid.
[234] Michael Barnett and Raymond Duvall, 'Power in International Politics' (2005) International Organization, 59:1 39, 45-57.
[235] ibid, 3-4.
[236] John Naughton, 'Good luck in making Google reveal its algorithm' *The Guardian* (London, 13 November 2016) <https://www.theguardian.com/commentisfree/2016/nov/13/good-luck-in-making-google-reveal-its-algorithm> accessed 9 December 2016.
[237] Carole Cadwalladr, 'Google, democracy and the truth about internet search' *The Guardian* (London, 4 December 2016, <https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook?CMP=share_btn_tw> accessed 9 December 2016.
[238] Michel Foucault, (n2), 178; Hille Koskela, 'Cam Era' – the contemporary urban Panopticon' (2003) Surveillance & Society 1:3 292, 299-300.
[239] Michel Foucault, (n2), 180-1, 246, 281.
[240] Connor Sheridan, (n64), 73.
[241] Paul Bernal, (n34), 249-250.

> compelling. Metaphors are instructive not for their realism but for the way they direct our focus to certain social and political phenomena.[242]

Sheridan highlights that because contemporary surveillance is often done without the knowledge of the subjects, Snowden had pulled back the curtain on the Panopticon. By destroying the illusion, Snowden reminded people that 'yes, there were provisions in place that certain powerful people had access to any sort of personal data they wanted about anyone in the country, to be accessed as they wished.'[243]

In relation to data retention and the Panopticon, Portela and Cruz-Cunha suggested that:

> … there is an analogy between the historical concept of the panopticon...and the retention of... data... [as]... the panopticon draws its power from the fact that the surveilled never know if they are surveilled... therefore *internalise habits* as if they were surveilled (author's emphasis).[244]

(d) Internalisation – The Panopticon and self-restraint/discipline and a rejection of Foucauldian critics

Manokha notes that much of the focus in surveillance studies has been on the domination/power aspect of the Panopticon, when this is not the only or even most important aspect.[245] Foucault himself acknowledging that '*it is only one aspect* of the art of governing people in our societies (author's emphasis).'[246] This focus on power and domination has led to a one-sided and limited interpretation, which has led to many (including Lyon above) dismissing it as being inadequate.[247] Manokha notes that as well as Bentham's Panopticon being about having power over an individual, it is also concerned with the power one exercises over themselves through self-discipline and restraint, making coercion unnecessary.[248] This unnecessary reliance on coercion is echoed by Foucault.[249] Foucault in *Discipline and Punish* and later works constantly referred to the Panopticon as resulting in self-restrain, self-objectification and becoming the principle of one's own subjection.[250] This as noted above has the effect of 'obtaining power of mind over mind' and what is known as the chilling effect, mentioned in this Chapter and discussed in detail in Chapter 4. This discussion need not be repeated here, but it is essential to note that Manokha observed that since the Snowden revelations which pulled back the curtain on the Panopticon there has been chilling effects in journalism, social media behaviour (online and offline), political opinions and identity expressions.[251] For said reasons, Manokha noted that the metaphor of the Panopticon is 'not

[242] Daniel Solove, *The Digital Person Technology and Privacy in the Information Age* (NYU Press 2006), 28.
[243] Connor Sheridan, (n64), 66.
[244] Irene Maria Portela and Maria Manuela Cruz-Cunha, 'What About the Balance Between Law Enforcement and Data Protection?' in Irene Maria Portela and Maria Manuela Cruz-Cunha (eds) *Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues*, (IGI Global 2010), 10.
[245] Ivan Manokha, 'Surveillance, Panopticism, and Self-Discipline in the Digital Age' (2018) Surveillance and Society 16:2 219, 220.
[246] Michel Foucault, 'Sexuality and solitude' in Marshall Blonsky (ed) *On Signs: A Semiotics Reader* (Blackwell, Oxford), 367.
[247] Ivan Manokha, (n245), 220-221.
[248] ibid, 222.
[249] Michel Foucault, (n2), 201.
[250] Ivan Manokha, (n245), 225-226.
[251] ibid, 229-230.

only…still relevant but it is actually more relevant today than with respect to Western societies of the nineteenth and twentieth centuries.'[252]

Taking this and the above into account, Portela further argued that data retention as being better described as 'panspectron.'[253]

5.7 From Panopticon to Panspectron?

The Panspectron was coined and distinguished from the Panopticon by Manuel DeLanda where he writes that a Panspectron '*compiles information about all at the same time*, using computers to select the segments of data relevant to its surveillance tasks (author's emphasis).'[254] This can include all information from the electromagnetic spectrum.[255] The Panspectron is concerned about mass surveillance and control.[256] Hookway[257] argued that the Panopticon had been replaced by the Panspectron. Building on this, Braman continues that:

> In a panspectron, no surveillance subject is identified in order to trigger an information collection process. Rather, information is collected about everything and everyone all the time. A subject appears only when a particular question is asked, triggering data mining in information already gathered to learn what can be learned in answer to that question. While in the panopticon environment the subject knows that the watcher is there, in the panspectron environment one may be completely unaware that information is being collected.[258]

Such lack of awareness was also noted by Sheridan[259] with Braman highlighting that the Panspectron was already a reality encompassing areas such as *electronic communications* and would continue to increase in other aspect of our lives unless effective legal barriers are re-enacted.[260] In addition to this it was highlighted that ISPs were pressured or required to maintain digital records of transactions and communications.[261] Although it was noted that data retention laws could be regarded as visible for Panoptic purposes, it cannot be assumed that *everyone* would know and to the *extent* such laws permit retention.

(a) Data retention is both Panoptic and Panspectric?

Considering both the Panopticon and the Panspectron, it is argued that for the purposes of data retention, this could theoretically be both. Dahan notes that Panoptical and Panspectral

---

[252] ibid, 230.
[253] Irene Maria Portela and Maria Manuela Cruz-Cunha, (n244), 10.
[254] Manuel DeLanda, *War in the Age of Intelligent Machines* (Swerwe Editions, New York, 1991), 205-206; Elisabeth Fura and Mark Klamberg, 'The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA' in Josep Casadevall, Egbert Myjer and Michael O'Boyle (eds) *Freedom of Expression: Essays in honour of Nicolas Bratza, President of the European Court of Human Rights* (Wolf Legal Publishers, Oisterwijk 2012), 463-481.
[255] Michael Dahan, 'The Gaza Strip as Panopticon and Panspectron: The Disciplining and Punishing of a Society' (2013) IJEP 4:3, 44.
[256] ibid.
[257] Branden Hookway, *Pandemonium: The rise of predatory locales in the postwar world* (Princeton, N.J.: Princeton Architectural Press 2000).
[258] Sandra Braman, 'Tactical memory: The politics of openness in the construction of memory' (2006) First Monday 11:7.
[259] Connor Sheridan, (n64), 48.
[260] Sandra Braman, (n258).
[261] ibid.

technologies are not mutually exclusive and can coexist.[262] Whether surveillance is Panoptic or Panspectric depends upon the awareness of the individual concerned. For example, data retention could be argued to be Panoptic because one is aware of Part 4 of the IPA 2016 and the retention notices that can be issued under it. Data retention could also, equally be argued to be Panspectric because it may not be known to the masses what *extent* data retention interferes with fundamental rights and the extent at which data is collected, aggregated for predictions. This can be further explored because under a retention notice, a telecommunications operator can be required to *generate* data, and it is this generation of data that would put an individual, even if they knew the ins and outs of Part 4 in the dark about just what data about them is being generated. In similar fashion, from a US perspective, Sheridan notes:

> The public was told that these surveillance activities were being carried out, and their data was subject to review by any authorized party. The problem was that the average citizen did not know the *extent* of said review. Many things that we assumed to be private were in fact open secrets to those with the right clearance.[263]

A far greater issue, however, is extent of the surveillance across the entire electromagnetic spectrum and the predictive use made of that data.

5.8 Other ideas of data collection/retention as surveillance

The Surveillance Studies Network maintained that 'where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance.'[264] This like Lyon refers to focussed surveillance and prediction. However, Marx had misgivings with dictionary definitions of surveillance as new technologies did not especially apply to a 'suspect' (i.e. focussed, see Oxford Living Dictionary above) but could apply to geographical places[265] and spaces, particular time periods, networks, systems and categories of person.[266] Marx highlights that a better definition of surveillance would be 'the use of technical means to *extract or create personal data* (author's emphasis).'[267] The relation to data retention in the IPA 2016 is quite similar in that data can be retained or created for further analysis. For Marx, new surveillance has low visibility, or is even invisible, it is involuntary, the data collection is often integrated into routine activity and is more likely to be automated involving machines rather than humans.[268] Marx continues that data collection is often carried out remotely by third parties in which the data can be available in real time, can be continuous and offer information on the *past*, *present* and *future*.[269] The subject of data collection goes beyond individual suspects[270] as would any obligation to retain as it is focussed on services used. Marx regards surveillance

[262] Michael Dahan, (n255).
[263] Connor Sheridan, (n64), 71.
[264] A report on the Surveillance Society for the Information Commissioner (September 2006) <https://www.york.ac.uk/res/e-society/documents/20061106surveillance.pdf> accessed 22 November 2015, para 3.1.
[265] *Tele2 Sverige AB and Watson*, (n40), [111].
[266] Gary Marx, 'What's New About the "New Surveillance"? Classifying for Change and Continuity' (2002) Surveillance & Society 1:1: 9, 10.
[267] ibid, 12.
[268] ibid, 15.
[269] ibid.
[270] ibid.

as a quest for information,[271] and this is true for data retention as the purpose is to keep information on a 'just in case' basis.

5.9 Data retention as surveillance, a legal perspective

(a) Data Retention as Surveillance in EU Law

From an EU law perspective, the idea that data retention is a form of surveillance is implied by the wording of Article 5(1) of the e-Privacy Directive. Article 5(1) requires Member States to prohibit the 'listening, tapping, *storage* or other kinds of interception *or surveillance of communications* and the *related traffic data* by persons other than users (author's emphasis).' This implies that storage of traffic data is a type of surveillance of communications. This is also reflected in Article 5 of the proposed e-Privacy Regulation.[272]

In *Digital Rights Ireland*[273] AG Cruz Villalón, opined that the DRD may cause a vague feeling of surveillance[274] and that retention allows retrospective scrutiny, thus establishing conditions for surveillance.[275] This is similar to what Williams and Johnson refer as reconstructive surveillance.[276] The Article 29 Data Protection Working Party (WP29) argued that general data retention *would make surveillance* that is authorised in exceptional circumstances the rule.[277]

(b) Data Retention as Surveillance under the ECHR

Under the ECtHR's case law, it was previously noted that e-mail and internet usage fall within the ambit of Article 8[278] and on numerous occasions has held that the *storage* of private information amounts to[279] or is akin to[280] secret surveillance. The GC in *Zakharov* noted that 'that the existence of practices permitting *secret surveillance* be established and that there was a reasonable likelihood that the security services had compiled and *retained information concerning his or her private life* (author's emphasis).'[281]Even where secret surveillance[282] is carried out by private bodies, a State is under positive obligations to protect and respect private life.[283] This, according to Judge Pinto de Albuquerque includes the '[u]nconsented collection, access and analysis of…communications, including metadata.'[284] On the same day, Pinto de Albuquerque also maintained that the DRD enabled surveillance capabilities.[285] Therefore, this

[271] ibid, 17.
[272] Committee on Civil Liberties, Justice and Home Affairs, 'Text of the compromise amendments' <https://drive.google.com/file/d/0Byeaj8v2GIOacnVwVlhqMWdUWFU/view> accessed 12 November 2017.
[273] Opinion of Cruz Villalón, (n120).
[274] ibid, [52].
[275] ibid, [72].
[276] Robin Williams and Paul Johnson, 'Circuits of Surveillance' (2004) Surveillance & Society 2:1 1, 4.
[277] Opinion 9/2004 of Article 29 Data Protection Working Party, (9 November 2004) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp99_en.pdf> accessed 22 November 2017.
[278] *Copland*, (n217), [41].
[279] *Rotaru v Romania* App no 28341/95 (ECHR, 4 May 2000), [41], [59]; *Segerstedt-Wiberg and Others v Sweden* App no 62332/00 (ECHR, 6 June 2006), [71], [76].
[280] *S and Marper*, (n23), [99].
[281] *Roman Zakharov*, (n16), [167].
[282] *Bărbulescu v Romania* App no 61496/08 (ECHR, 12 January 2016), see partly dissenting opinion of Judge Pinto de Albuquerque, [16-18].
[283] [52-54].
[284] *Szabo and Vissy*, (n102), [13].
[285] ibid, [15].

supports the idea, from an ECHR perspective that retention, whether by public or private entities constitutes surveillance.

(c) Data Retention as Surveillance in UK law

In *Davis and Watson*, the English Divisional Court distinguished *Kennedy v United Kingdom* from *Digital Rights Ireland* in that the former concerned an individual warrant of interception issued by the Secretary of State while the latter concerned a general data retention regime on a potentially massive scale.[286] The Court of Appeal referred to this distinguishing feature and held that the former 'was concerned with an individual warrant and *not mass surveillance* (author's emphasis),'[287] therefore, clearly indicating that 'data retention is mass surveillance.'[288]

A legal UK definition for surveillance can be found in s.48(2) of the RIPA 2000 which 'includes' (and therefore not limited to):[289]

1. monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;
2. recording anything monitored, observed or listened to in the course of surveillance; and
3. surveillance by or with the assistance of a surveillance device.

'Communication' for the purposes of s.81(1)(b) and (c) RIPA 2000 includes *data of any description* and signals between persons, persons and things, and things and things. This has been replicated in s.261(2)(a) and (b) of the IPA 2016. It is plausible to argue said definitions are Panspectric. Thus, communications data would fall within the ambit of s.48(2). This implies that the monitoring or observing, any recording of such monitoring in the course of surveillance or by a surveillance device of communications data is to be treated as surveillance. In addition to this, s.81(1) defines person as any organisation and any association or combination of persons and so surveillance does not need to be targeted at any one individual to constitute surveillance, it can thus constitute *mass* surveillance. The definition of 'person' is what allowed interception to be carried out in bulk in the so called 'thematic warrants.'[290]

Further elaboration on construing the definition of surveillance comes from the Investigatory Powers Tribunal (IPT) in *Vaughan v South Oxfordshire District Council*.[291] Here, the IPT held that 'the way in which s48(2) is drafted means that *conduct which has as its purpose such monitoring or observation would be surveillance within the meaning of the act, even if no actual monitoring of any persons took place* (author's emphasis).'

The IPT placed great emphasis on purposes. It is clear that the purpose of data retention is to aid in the interests of national security, the purposes of preventing or detecting crime or of

[286] *Davis & Ors, R (on the application of) v Secretary of State for the Home Department & Ors* [2015] EWHC 2092, [81].
[287] *Davis & Ors, R (on the application of) v Secretary of State for the Home Department & Ors* [2015] EWCA Civ 1185, [114].
[288] Matthew White, 'Protection by Judicial Oversight, or an Oversight in Protection?' (2017) Journal of Information Rights, Policy and Practice 2:1 1, 34.
[289] Simon McKay, 'Defining Surveillance' (22 January 2016) <https://simonmckay.wordpress.com/2016/01/22/defining-surveillance/> accessed 22 November 2017.
[290] See the interpretation of 'person' in s.8(1) See Intelligence and Security Committee, *Privacy and Security: A modern and transparent legal framework* (2014, HC 1075), 42-45.
[291] *Vaughan v South Oxfordshire District Council* [2012] IPT/12/28/C, [16-19].

preventing disorder and many more. Therefore, even if one is to argue that data retention itself is not surveillance, the conduct of data retention allows for the access of communications, which consequently enables the monitoring of communications data, as AG Cruz Villalón in *Digital Rights Ireland* pointed out, it establishes the conditions for surveillance. Even if that data is never accessed, the purpose for data to be retained, remains unchanged, and consequently the conduct of retention still enables it to fall within the definition of surveillance. If one were to argue that data retention is not monitoring or observing, then this is countered by the 'recording' element of s.48(2). Recording in this context should be given a broad interpretation such as pen and paper[292] as surveillance is inclusive, not exclusive and should therefore apply to the capturing of data inherent in data retention.

In *Re: a complaint of surveillance*,[293] the IPT drew some conclusions about the definition of surveillance in that it is essentially an *intelligence gathering activity* involving various means which is not constrained by 'surveillance in ordinary English usage.' Section 48(2) may operate to amplify the ordinary meaning, thus identifying particular aspects of intelligence gathering without expressly defining surveillance itself, or providing when or where it takes place, or who is conducting it.

The IPT's reasoning demonstrates just how broad the definition of surveillance can be. If the purpose of data retention is to gather intelligence i.e the communications data of persons, then based on the IPT's reasoning, the retention process itself is essentially surveillance. The various means by which surveillance can be conducted leaves it open to suggestion that data retention could fall within this ambit, as the IPT did not define those various means, it in fact left it open as potentially going beyond the ordinary English meaning.

Regarding surveillance devices, the then Chief Surveillance Commissioner, Sir Christopher Rose noted that the 'Internet is a surveillance device as defined by RIPA section 48(1) [means any apparatus[294] designed or adapted for use in surveillance.'[295] If this contention is correct, then any monitoring, observing, recording of internet activity would constitute surveillance by a surveillance device, and would thus again put data retention within the ambit of surveillance. One could argue that the use of a surveillance device could be argued further, if one considers the devices that actually *enable* the retention of communications data. One could even delve deeper into the issue of surveillance devices. For example, Cisco's Netflow Auditor[296] can allow real time or long term historical visibility of every network flow recorded.[297] Rafi Sabel argues that Netflow Auditor is the solution to assist 'ISP's to quickly comply at a low cost *whilst properly allowing data retention rules* to be implemented' (author's emphasis).[298] So in a broad and narrow sense, the ability to retain data can constitute a surveillance device. Section 48 is silent on data retention and given the inclusive definition of surveillance, there is nothing to suggest that it *is not*. It has been suggested that data retention can satisfy all three aspects of s.48(2).

---

[292] Martin Tunley, Andrew Whittaker, Jim Gee and Mark Button, *The Accredited Counter Fraud Specialist Handbook* (John Wiley & Sons 2014), 76.
[293] *Re: a complaint of surveillance* [2013] IPT/A1/2013, [12-14].
[294] includes any equipment, machinery or device and any wire or cable; s.81(1) RIPA 2000.
[295] Annual Report of the Chief Surveillance Commissioner, HC 498 SG/2012/127, para 5.18.
[296] Netflow Auditor <http://www.netflowauditor.com/> accessed 23 November 2017.
[297] Netflow Auditor <http://netflowauditor.com/details.php> accessed 23 November 2017.
[298] Rafi Sabel, 'How NetFlow Solves for Mandatory Data Retention Compliance' (8 August 2016) <http://blog.netflowauditor.com/how-netflow-solves-for-data-retention-compliance> accessed 16 December 2016.

5.10 Data Retention as Mass Surveillance

Now that it has been argued that theoretically and legally, data retention is a form of surveillance, it is important to consider whether it also constitutes mass surveillance. Roger Clarke, suggested that the primary purpose of surveillance was to *collect* information about individuals or *en masse*.[299] Clarke subsequently highlighted that '[d]ata retention proposals...*are unequivocally a weapon of mass surveillance'* (author's emphasis).[300] In the House of Lords Select Committee on the Constitution's 2nd Report titled Surveillance: Citizens and the State[301] it was understood that there were two broad types of surveillance, mass surveillance and targeted surveillance. Mass surveillance also termed 'passive' or 'undirected' surveillance is not targeted on any particular individual *but gathers information* for possible future use.[302]

Roberts and Palfrey argues[303] that the monitoring amounts to surveillance. Not in the traditional sense, but due to its functional similarities, by requiring the collection of data about citizens without their consent, enabling the state to use data to control some of the subjects of monitoring. Stalla-Bourdillon maintains that 'the systematic character of the collect, as well as its scope, and its possible uses that are at the core of mass surveillance techniques.' Stalla-Bourdillon continues that 'they are imposed [as] a general monitoring duty which consists of *gathering and retaining information about their users* (author's emphasis).'[304] The logical conclusion that can be drawn from this is that if data retention is surveillance, then general data retention obligations must be classified as mass surveillance.

5.11 Surveillance within surveillance

Regarding the Panopticon, Lyon highlights the impression Foucault gives 'that citizens of modern nation-states find themselves increasingly to be the subjects of centralised carceral discipline.'[305] Richards notes that due to the blurring of public and private surveillance practices, models of understanding surveillance such as the Panopticon are the most out of date.[306] But to suggest that Foucault *only focussed* on centralised surveillance is to mischaracterise his position. Foucault noted that the Panopticon 'is a marvellous machine which, *whatever use one may wish to put it to*, produces homogeneous effects of power' (author's emphasis).[307] Foucault continued that the Panopticon could be utilised by anyone (or

---

[299] Roger Clarke, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms' (1997) <http://www.rogerclarke.com/DV/Intro.html> accessed 29 November 2016.
[300] Roger Clarke, 'Data retention as mass surveillance: the need for an evaluative framework' International Data Privacy Law (2015) 5 (2): 121-132, p127.
[301] House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State. Volume I: Report* (second report) (2008–09, HL 18–I).
[302] ibid, para 24.
[303] Hal Roberts and John Palfrey, 'The EU Data Retention Directive in an Era of Internet Surveillance' in Ronald J. Deibert and others (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (MIT Press 2010), 36.
[304] Sophie Stalla-Bourdillon, 'Online monitoring, filtering, blocking….What is the difference? Where to draw the line?' (2013) Computer law & security review 29:6 702, 708.
[305] David Lyon, (n212).
[306] Neil Richards, (n76), 1940-1941, 1958-1959; William Bogard, 'Surveillance assemblage and lines of flight' in David Lyon (ed) Online monitoring, filtering, blocking Online monitoring, filtering, blocking *Theorizing surveillance: The Panopticon and Beyond* (Portland, OR: Willan 2006), 102; Susanne Lace, 'The new personal information agenda' in Susanne Lace (ed) *The Glass Consumer* (Birstol: Policy Press 2005), 210; Manuel Castells, *The power of identity* (Malden, MA: Blackwell 2004), 342; Daniel Solove, (n242), 32.
[307] Michel Foucault, (n2), 202.

society as a whole) for any purpose.[308] As can the Panspectron, if one considers the Gaza strip.[309]

Fuchs is also in agreement where he added that 'Foucault's analysis does not exclude that the methods of surveillance can become more decentralized and dispersed because'[310] surveillance is a '…network of relations from top to bottom, but also to a certain extent from bottom to top and laterally.'[311] The latter, in which can be termed 'Sousveillance'[312] can be regarded as surveillance of citizens *by* citizens or institutions,[313] which has been explored to some extent by Mark Andrejevic.[314]

Mitrou also noted the technique of folding private organisations into government surveillance networks creates a system of 'distributed surveillance' which allows the state to overcome practical limits on its resources.[315] Using Foucault's ideas of surveillance and discipline[316] Boyle highlights examples in the United States where 'the state has worked actively to embed or hardwire the legal regime in the technology itself'[317] by various means such as being mandated by law.[318] This is true for the UK also where the state can require intercept capabilities, and require the development of practices in which data can be retained. Boyle warned that if digital technologies enlarge our space for living, the dangers posed by that expansion will prompt a reasonable demand 'that the Panopticon be hardwired into the "technologies of freedom'[319] (becoming more Panspectric) that enable freedom of expression.[320]

Ogura argued that 'the common characteristics of surveillance are the management of population based on capitalism and the nation state.'[321] Shoshana Zuboff coins the term 'Surveillance Capitalism' in which 'profits derive from the unilateral surveillance and

[308] ibid, 207, see also 215 and 216.
[309] Michael Dahan, (n255).
[310] Christian Fuchs, (n49), 119.
[311] Michel Foucault, (n2), 176; See references made to 'horizontal visibility' in Martin Berner, Enrico Graupner and Alexander Maedche, 'The Information Panopticon in the Big Data Era' (2014) Journal of Organization Design 3:1 14, 16.
[312] Steve Mann, Jason Nolan and Barry Wellman, 'Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments' (2003) Surveillance & Society 1:3 331.
[313] ibid, 335-336.
[314] Mark Andrejevic, 'The work of watching one another: Lateral surveillance, risk, and governance' (2005) Surveillance & Society 2:4 479; Mark Andrejevic, *iSpy: Surveillance and power in the interactive era* (Lawrence, KA: University Press of Kansas 2007); Mark Andrejevic, 'Privacy, exploitation, and the digital enclosure' (2009) Amsterdam Law Forum 1:4 47.
[315] Lilian Mitrou, (n158), 141.
[316] James Boyle, 'Foucault in cyberspace' (1997) University of Cincinnati Law Review 66:1 177, 186.
[317] ibid, 188.
[318] ibid.
[319] ibid.
[320] Ithiel de Sola Pool, *Technologies of Freedom* (Belknap Press; Reprint edition 1984).
[321] Toshimaru Ogura, 'Electronic government and surveillance-oriented society' in David Lyon (ed) *Theorizing surveillance: The Panopticon and Beyond* (Portland, OR: Willan 2006), 272.

modification of human behaviour.'[322] And just like the Panopticon, surveillance capitalism seeks to reward and punish.[323]

Oscar Gandy would describe this as the 'Panoptic Sort' which is 'a technology that has been designed and is being continually revised to serve the interests of decision makers within the government and the corporate bureaucracies.'[324] Gandy concluded that this created 'an antidemocratic system of control that cannot be transformed because it can serve no purpose other than that for which it was designed—the rationalization and control of human existence.'[325]

Sullivan builds upon Gandy's Panoptic Sort for contemporary purposes in light of the Snowden revelations.[326] Sullivan points to the likes of Google, Twitter, and Facebook being the Panoptic Sort to which Gandy's work identified, in some instances having both legal and *financial* interests in handing over sensitive personal information to government agencies. This is also reflected in the IPA 2016 in relation to reimbursing the costs of retaining Internet Connection Records but that is not really an incentive, more a reimbursement of expenses.[327] Sullivan concluded without transparency in the ways in which governments and corporations gather, store and search our data, the data Panopticon will persist.[328] This begins to demonstrate the term of 'surveillance within surveillance' in relation to data retention, in which private corporations initially conduct surveillance for their own purposes and *then* such surveillance becomes subject to state control i.e. retaining the seeds of said prior surveillance.

The Panoptic Sort was also regarded as a difference machine that sorts individuals into categories and classes on the basis of routine measurements. Gandy regarded this as a discriminatory technology which allocates options and opportunities on the basis of those measures and the administrative models that they inform good. This system of power and

---

[322] Shoshana Zuboff, 'The Secrets of Surveillance Capitalism' (5 March 2016) <http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html> accessed 22 February 2017; Andrew Ledvina, '10 ways Facebook is actually the devil' (4 July 2014) <http://andrewledvina.com/code/2014/07/04/10-ways-facebook-is-the-devil.html> accessed 25 November 2017, 'The fundamental purpose of most people at Facebook working on data is to influence and alter people's moods and behaviour. They are doing it all the time to make you like stories more, to click on more ads, to spend more time on the site'; Noam Scheiber, 'How Uber Uses Psychological Tricks to Push Its Drivers' Buttons' *New York Times* (New York City, 2 April 2017) <https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html?smid=tw-share&_r=0> accessed 25 November 2017; Robert M. Bond, Christopher J. Fariss, Jason J. Jones, Adam D. I. Kramer, Cameron Marlow, Jaime E. Settle and James H. Fowler, 'A 61-million-person experiment in social influence and political mobilization' (2012) Nature 489 295; Adam D. I. Kramera, Jamie E. Guillory, and Jeffrey T. Hancockb, 'Experimental evidence of massive-scale emotional contagion through social networks' (2014) 111:24 8788; Jaron Lanier, 'Should Facebook Manipulate Users?' *The New York Times* (New York City, 30 June 2014) <https://www.nytimes.com/2014/07/01/opinion/jaron-lanier-on-lack-of-transparency-in-facebook-study.html> accessed 25 November 2017; Jonathan Zittrain, 'Facebook Could Decide an Election Without Anyone Ever Finding Out' *The New Republic* (New York City, 2 June 2014) <https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering> accessed 25 November 2017.

[323] Shoshana Zuboff, (n90), 82.

[324] Oscar Gandy, *The panoptic sort. A political economy of personal information* (Boulder: Westview Press 1993), 95.

[325] ibid, 227.

[326] John Sullivan, 'Uncovering the data panopticon: The urgent need for critical scholarship in an era of corporate and government surveillance' (2013) The Political Economy of Communication 1:2.

[327] Science and Technology Committee, *Investigatory Powers Bill: technology issues (third report)* (2015–16, HC 573), 23-26.

[328] John Sullivan, (n326).

disciplinary surveillance identifies, classifies and assesses.[329] Fuchs draws a Panoptic sort analogy with Facebook[330] and concludes that it is a form of surveillance that *exerts power and domination* by making use of specific qualities of the contemporary Internet, such as user-generated content and permanent dynamic communication flows.[331]

A decentralised Panopticon may also have a legal basis. In Europe, this takes its form from data protection laws.[332] These laws regulate the processing of personal data by data controllers.' At an EU and UK level, data controllers can process data without consent if it serves a legitimate interest such as marketing,[333] or another legal basis, and this is what allows companies such as Google and Facebook to accumulate vast amounts of data. Former CEO of Google, Eric Schmidt once said:

> In a world of asynchronous threats, it is too dangerous for there not to be some way to identify you. We need a [verified] name service for people. Governments will *demand it* (author's emphasis).[334]

In regards to data retention, telecommunications operators can be compelled to retain and generate (Big and other) data, surveillance within surveillance. Fuchs concludes that surveillance today is not Panoptic because surveillance technologies are centralised and hierarchic but because states and corporations are dominant actors that accumulate power that they can use for disciplinary surveillance.[335]

5.12 Conclusions

This Chapter has sought to demonstrate from theoretical and legal perspectives, why communications data retention should be regarded as secret mass surveillance within surveillance. This has been achieved by considering theories of surveillance and concluding that data retention can be both Panoptic, and Panspectric. The Panopticon, popularised by Faucoult highlighted that disciplinary power is not about acts of physical violence (just as Jacobs notes with regards to totalitarian societies),[336] it trains, drills and normalises people[337] turning them docile,[338] inducing the chilling effect. It is unsurprising that Foucault's work on power is regarded as mattering more than ever today.[339]

---

[329] Oscar Gandy, (n324), 15. See discussion on 'social sorting' in Chapter 5 and Big Data discrimination in Chapters 4 and 5.
[330] Christian Fuchs, (n229), 134.
[331] ibid, 145.
[332] Michael Rhoen, (n231), 2.
[333] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (9 April 2014) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 23 November 2017, 25.
[334] Marshall Kirkpatrick, 'Google CEO Schmidt: "People Aren't Ready for the Technology Revolution"' (4 August 2010) <http://readwrite.com/2010/08/04/google_ceo_schmidt_people_arent_ready_for_the_tech/> accessed 4 December 2016.
[335] Christian Fuchs, (n49), 120-121.
[336] See Chapter 1.
[337] Colin Koopman, 'The Power Thinker' (15 March 2017) <https://aeon.co/essays/why-foucaults-work-on-power-is-more-important-than-ever?utm_content=buffer25bb6&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer> accessed 8 January 2018.
[338] Michel Foucault, (n2), 135-141.
[339] Colin Koopman, (n337).

In addition to this, the ECHR, EU and UK law also demonstrate that data retention is a form of surveillance, based on jurisprudence and statutes. Moreover, the synergy between governments and private corporations highlighted the dual surveillance nature whereby the latter would conduct their own surveillance (allowed by national law) and give the former subsequent control, or the former would mandate surveillance for subsequent control creating what has been coined surveillance within surveillance. As Foucault accepted, 'that there were real forces of violence in the world, and not only state violence. There is also corporate violence due to enormous condensations of capital.'[340] General consensus from focus groups have demonstrated that 'that the collection of metadata is seen as surveillance.'[341] Reasons for this centred around:

> [I]deas such as giving consent for data collection, personal ownership of data, questions around why this data would need to be collected, the lack of anonymity and the ability to be identified by the collection of [useful] metadata.[342]

It has been recommended that the UK government take views of the public into account on digital surveillance and privacy and would have to do more to persuade the public that bulk data collection is anything but mass digital surveillance.[343] Moreham notes that '[b]ecause information collection and storage is regarded as a form of surveillance, Art.8(2) is applied strictly in these cases'[344] highlighting why the same strict standards of interception must apply to data retention.[345]

This Chapter avoided defining surveillance itself as the focus was placed upon data retention. Constructing a definition of surveillance based on a specific type of surveillance measure may have had the unintended consequence of defining it too narrowly. Haggerty and Samatas have noted the difficulty scholars face when making generalisations about surveillance because of the different dynamics and implications of various types.[346] This approach was adopted by Foucault, who declined to define power because people would win more freedom by declining to define in advance 'all the forms that freedom could possibly take.'[347] Thus, the metaphor of the Panopticon was used to demonstrate how best to describe data retention as surveillance. Moreover, relying upon the dictionary and Lyon's definition of surveillance proved to be too narrow in themselves.

In arguing that data retention can be Panoptic, McMullan asks in the world of digital surveillance and data capture are we still objects of information?[348] McMullan continues that in the 'private space of my personal browsing I do not feel exposed – I do not feel that my body

---

[340] ibid.
[341] A Report by DATA-PSST and DCSS, 'Public Feeling on Privacy, Security and Surveillance' (November 2015) <https://sites.cardiff.ac.uk/dcssproject/files/2015/11/Public-Feeling-on-Privacy-Security-Surveillance-DATAPSST-DCSS-Nov2015.pdf> accessed 13 January 2017, p8.
[342] ibid.
[343] ibid, p5.
[344] Nicole Moreham, 'The right to respect for private life in the European Convention on Human Rights: a re-examination' (2008) EHRLR 1 44, 64.
[345] See Chapter 3.
[346] Kevin D. Haggerty and Mina Samatas, 'Surveillance and democracy: an unsettled relationship' in Kevin D. Haggerty and Mina Samatas (eds), *Surveillance and Democracy* (Routledge-Cavendish (2010), 3.
[347] Colin Koopman, (n337).
[348] Thomas McMullan, 'What does the panopticon mean in the age of digital surveillance?' *The Guardian* (London, 23 July 2015) <https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham> accessed 18 December 2016.

of data is under surveillance because I do not know where that body begins or ends.' McMullan articulates that due to the anonymity of the internet, rather than normalising behaviour, the opposite happens. McMullan argues that due to the Internet of Things (IoT), the interconnectivity of regular objects (cars, homes, even sex objects)[349] via the internet, the vast data created about our lives will most likely 'wind its way towards corporate and government reservoirs.' McMullan highlights that there may not be a communicating tower, but there will be communicating sensors in our most intimate objects. The idea of the IoT becomes important in the question on to whom an obligation to retain can be imposed upon as we move closer to an all-encompassing Panspectron.

[349] David Kravets, 'Maker of Internet of Things-connected vibrator will settle privacy suit' *Ars Technica* (8 December 2016) <http://arstechnica.com/tech-policy/2016/12/maker-of-internet-of-things-connected-vibrator-will-settle-privacy-suit/> accessed 18 December 2016.

Chapter 6: Who is obligated to retain? Everything that 'communicates'?

6.1 Introduction

This Chapter considers what types of communication service providers are under an obligation to retain communications data. Although the UK has voted to leave the European Union (EU), it is still a Member State and thus EU law still applies as would any retained EU law. The Article 29 Data Protection Working Party (WP29) (created by Directive 95/46/EC to provide independent advice to the European Commission on data protection matters)[1] expressed its hesitancy to impose retention obligations *on a wider number of communications service providers* because it was felt unnecessary (author's emphasis).[2] The WP29 also stressed that the European Commission must ensure that when extending the scope of the new e-Privacy instrument, this should not automatically allow Member States to bring new communication services in the scope of new or existing national data retention legislation.[3] The WP29 did not expand upon why such restraint was necessary, but the UK has exercised none. This Chapter will demonstrate the implications of adding retention obligations to new communications service providers.

The obligation to retain communications data under EU law lies with publicly available electronic communications services.[4] The UK uses its own terminology of what were once public telecommunications services, and are now telecommunications operators. This Chapter discusses the definitions of electronic communications services/networks and telecommunications services/systems/operators whilst also highlighting the public and private element, with the latter increasing the scope of retention obligations. This Chapter also concerns itself with the evolution of who could be obliged to retain from public telecommunications services to telecommunication operators which now includes both telecommunication services *and* telecommunication systems, removing the public barrier which was once present. This signifies the UK's extension beyond EU law to include essentially anything that can communicate across *any* network i.e. WiFi, Bluetooth, the devices themselves that enable communications, software, apps, websites etc, emerging networks and services and devices, and devices related to the Internet of Things (IoT). This will highlight how the IoT will bring about interferences with the 'family life' and 'home' aspect of Article 8 of the European Convention on Human Rights (ECHR) relating back to Chapter 4. Furthermore, this Chapter will demonstrate that under the Investigatory Powers Act 2016 (IPA 2016) the power *to* obligate retention does not just fall upon the Secretary of State and Judicial Commissioner but on public authorities and others. The obligation to retain could essentially capture anything that communicates ever, and therefore be imposed on *anyone*.

6.2 What does European Union and UK Law have to say?

a. EU law

[1] Glossary <https://edps.europa.eu/data-protection/data-protection/glossary/a_en> accessed 30 November 2017.
[2] Article 29 Data Protection Working Party, 'Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)' (July 2016) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf> accessed 21 October 2016, p8.
[3] ibid.
[4] Article 3(1) and 15(1) of Directive 2002/58/EC (the e-Privacy Directive).

Article 15(1) of Directive 2002/58/EC (Directive on privacy and electronic communications, the e-Privacy Directive) allows Member States to adopt legislative measures providing for the retention of data for a limited period justified on the grounds such as national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. Article 3(1) sets out that retention obligations apply to publicly available electronic communications services (ECS) in public communications networks (PCN).

Article 2(c) of Directive 2002/21/EC defines ECS as a service which consists wholly or in part in the conveyance of signals on networks. This excludes broadcasting services which exercise editorial control over content, and information society services (ISS). An ECS would be an Internet Service Provider (ISP) such as TalkTalk using BT's network (PCN) but not internet telephony (VoIP) or e-mail and instant messaging providers,[5] demonstrating the limited[6] scope of who could be obligated to retain. This is further restricted by the 'publically available' element meaning any ECS that is provided so as to be available for use by members of the public.[7] Due to ECS not covering ISS (which are over the top services (OTT)) this would exclude services like Skype, Google search, Whatsapp and Netflix[8] from retention obligations when said services do not wholly or mainly concern itself with the conveyance of signals and content services. Brown does however point to an interesting conflict of interpretation, Recital 20 of the e-Privacy Directive imposes obligations on service providers who offer publicly available electronic communications services *over* the Internet. He opines that if a provider is offering a service "over the Internet," that service does not consist in the conveyance of signals, and instead, on the basis of the definitions, would be an ISS.[9] However, where there is a conflict between a preamble and a Community act, the latter takes precedence.[10] Moreover, many services over the internet can be purely content based services (Netflix), thus again outside the definition of ECS.

b. The Regulation of Investigatory Powers Act 2000 (RIPA 2000)

Under the old regime of RIPA 2000, retention obligations were imposed on public telecommunications services. Telecommunications services fall under the category of communications service providers (CSPs).[11] The meaning of a telecommunications service can be found in s.2(1) and s.81(1) RIPA 2000 which states that any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system

[5] Article 29 Data Protection Working Party, (n2), p5.
[6] G. Odinot, D. de Jong, R.J. Bokhorst and C.J. de Poot, 'The Dutch implementation of the Data Retention Directive' (2014) <https://www.wodc.nl/binaries/ob310a-full-text_tcm28-78190.pdf> accessed 9 August 2017, p136.
[7] Section 151(1) of the Communications Act 2003.
[8] European Parliament, 'Regulating electronic communications A level playing field for telecoms and OTTs?' (September 2016) <http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/586641/EPRS_BRI%282016%29586641_EN.pdf> accessed 30 November 2017, p2 and 4.
[9] Neil Brown, 'An assessment of the proportionality of regulation of 'over the top' communications services under Europe's common regulatory framework for electronic communications networks and services' (2014) Computer Law & Security Review 30:4 357, 360.
[10] Case-162/97 *Nilsson & Ors (Agriculture)* [1998] ECR I-7477, [54]; Case-308/97 *Manfredi (Agriculture)* [1998] ECR I-7685, [30]; Allan Littler, *Member States versus the European Union: The Regulation of Gambling* (Martinus Nijhoff Publishers 2011), 298.
[11] Home Office, 'Acquisition and Disclosure of Communications Data Code of Practice' (March 2015) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf> accessed 30 November 2017, para 1.5.

(whether or not one provided by the person providing the service); and "telecommunication system" means any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy (see Smith's example below). This can be subdivided into public and private telecommunication systems. Private telecommunication systems are telecommunication systems which without itself being a public telecommunication system are systems that are attached, directly or indirectly and whether or not for the purposes of the communication in question, to a public telecommunication system and its apparatus is both located in the UK and used for making the attachment to the public telecommunication system. As Barclay notes that '[s]ection 1 goes beyond section 1 of the Interception of Communications Act 1985 which the current Act repeals, by the inclusion of private telecommunications service.'[12]

This, however, was done in response[13] to *Halford v UK* where the European Court of Human Rights (ECtHR) discovered that Interception of Communications Act 1985 (ICA 1985) did not apply to internal communications operated by public authorities nor were there any provisions in other domestic law which regulated interception made on such systems.[14] Reid and Ryder, echoed by Benjamin[15] summarised this by stating this inclusion of private telecommunications systems is required in order guarantee that provisions of RIPA 2000 extend to the internet as access to the internet is generally provided by private organisations, thus putting ISPs within the ambit of RIPA 2000.[16] Smith in support of this assertion pointed out that private telecommunication systems are likely to catch any private network where it is possible to send and receive emails, which would include most office networks.[17]

This assertion that telecommunication systems includes the internet requires some clarification by describing what the internet is in basic terms. According to the Federal Networking Council (FNC),[18] the internet is a global information system that:

(i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons;
(ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and
(iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

[12] Christopher Barclay, House of Commons Library Research Paper 00/25 'The Regulation of Investigatory Powers Act' (March 2000) <http://researchbriefings.files.parliament.uk/documents/RP00-25/RP00-25.pdf> accessed 30 November 2017, p26.
[13] Regulation of Investigatory Powers Bill Deb 12 Jun 2000, Column 1421.
[14] *Halford v UK* App no. 20605/92 (ECHR, 25 June 1997), [51].
[15] Okechukwu Benjamin Vincents, 'Interception of internet communications and the right to privacy: an evaluation of some provisions of the Regulation of Investigatory Powers Act against the jurisprudence of the European Court of Human Rights' (2007) E.H.R.L.R. 6 637, 639.
[16] Alan S. Reid and Nicholas Ryder, 'For Whose Eyes Only? A Critique of the United Kingdom's Regulation of Investigatory Powers Act 2000' (2001) Information & Communications Technology Law 10:2 179, 184.
[17] Graham Smith, *Internet Law and Regulation* (Sweet and Maxwell 4th edn 2007), 411.
[18] Federal Networking Council Resolution, 'Definition of the 'Internet,' (24 October 1995) <https://www.nitrd.gov/fnc/Internet_res.aspx> accessed 30 November 2017.

In simple terms, the Internet Protocol (IP) transfers data[19] over a network of computers (the internet) from sender to receiver, which are identified by an (IP) address[20] that is allocated to both.[21] This is similar to posting a letter as it requires at least a destination address for the postal services to deliver to.[22] The transmission of data can occur over wired or wireless networks which use electrical signals or electromagnetic waves.[23]

Reid and Ryder (and Fenwick) pointed to a deficiency with the definitions of telecommunication systems, notably that new technology may mean that some systems are completely outside the ambit of the Act, for example certain internal intranet systems used by commercial organisations.[24] Smith further elaborates this point by referring to the Explanatory Notes of RIPA,[25] Smith highlights the distinction between an office network, linked to a public telecommunication system by a private exchange and secure office intranet, the former falling within the definition of private telecommunications system and the latter is not. Smith regards the reference to secure office intranet as 'puzzling' because according to the definitions of a private telecommunications system a secure intranet would only fall outside this if it were completely physically isolated from the public network.[26] Smith also refers to the comments of Charles Clarke (the then Home Secretary) regarding the public-private distinction where he stated:[27]

> …on the matter of public-private systems and domestic systems…we believe, that domestic systems are unequivocally private systems. The end of the public system is the network termination point, which is usually the white BT box… Any extensions after that, whether to the PC or anything else, are part of the householder's private system.[28]

Smith suggests that although Clarke's explanation is in accordance with established distinctions between public and private networks, it does not reflect what is said in RIPA 2000 itself. Smith elaborates on this point by referring to one of the ingredients under RIPA 2000 is whether any public telecommunications service is provided by means of any part of the system.[29]Smith notes as s.2(1) of RIPA 2000 states that any service that consists in the provision of access to any telecommunication system which leads Smith to conclude that if offered or provided to a substantial section of the public, it becomes a public telecommunications service.[30] Smith's example which refers to an individual in an household who were to host a website or a collection of MP3 files on a domestic PC, or store webcam

---

[19] Implement Basic Networks and Security <http://www.sqa.org.uk/e-learning/HardOSEss04CD/page_10.htm> accessed 30 November 2017.
[20] William Stewart, 'Living Internet, How the Internet Works' <http://www.livinginternet.com/i/iw.htm> accessed 30 November 2017.
[21] Marina Del Rey, 'Internet Protocol, RFC 791' (1981) <http://www.rfc-editor.org/rfc/rfc791.txt> accessed 30 November 2017.
[22] Note that the senders address is not compulsory for the delivery of the letter.
[23] Wen-Chen Hu, *Multidisciplinary Perspectives on Telecommunications, Wireless Systems, and Mobile Computing* (IGI Global 2013).
[24] Alan S. Reid and Nicholas Ryder, (n16), 181; Helen Fenwick, *Civil Liberties and Human Rights* (4th edn Routledge-Cavendish 2009), 1034.
[25] Explanatory notes to RIPA 2000, para 27.
[26] Graham Smith, (n17), 411.
[27] ibid.
[28] Regulation of Investigatory Powers Bill Deb 16 March 2000.
[29] Graham Smith, (n17), 412.
[30] ibid.

pictures and make them available through the domestic phone line.[31] Smith suggests that, on the face of it this would appear to constitute offering the public access to the system consisting of the domestic PC (especially now due to the rise of home-workers and small businesses being run from the home).[32] Smith went on to point out that if apparatus used for the provision of hosting services is to be regarded as apparatus for the purpose of facilitating the transmission of communications within the definition of telecommunications systems, this would render the parts of the domestic system used for that purpose a public telecommunications system for the purposes of RIPA 2000.[33] If one looks to RIPA 2000 s.81, the definition of apparatus, this includes any equipment, machinery or device and any wire or cable, where the PC could fall under equipment, machinery or device, and the facilitating the transmission of communications could be the web hosting/MP3 storing. What Smith is arguing is that the web-hoster is not the telecommunication service, but *is* the telecommunication system. This would also apply to content and application providers such as Google, Facebook, Yahoo!, Microsoft, Tencent, Alibaba, Baidu, Amazon, eBay, Netflix, and Apple[34] and even ISPs themselves.[35] In order to store and process their content, these content and application providers require investment in data centres which contain thousands of metal racks, powerful computers (severs) or devices for data storage.[36] This equipment, just like Smith's web hosts PC would fall under apparatus for the purposes of s.81 and would thus be public telecommunication systems. This, however, would mean that the obligation to retain cannot be imposed in instances such as these because they are not public telecommunication *services*.[37] This demonstrates that the obligation to retain under RIPA 2000 and the e-Privacy Directive are very similar in that they are mostly concerned with ISPs and not OTT services.

c. Communications Act 2003

The Communications Act 2003 (CA 2003) replaced certain sections of the Telecommunications Act 1984 (TA 1984). Notably Schedule 3, para 5(b) states that 'the words "telecommunication services", wherever occurring, there shall be substituted "electronic communications services."' The ICA 1985 also used the term telecommunications service interchangeably with the TA 1984.[38] This would imply telecommunications services and ECS are to some degree to be treated as one and the same under UK law, therefore making it necessary to consider the CA 2003. This can be supported by Ofcom's general conditions guidelines, where they assert there are three main types of service providers. The first are ECS or networks which include both public and private networks, mobile and fixed (unless

[31] ibid.
[32] Flexibility, 'Home is where the start-up is' <http://www.flexibility.co.uk/flexwork/location/home-enterprise.htm> accessed 30 November 2017.
[33] Graham Smith, (n17), 412.
[34] Analysis Mason, 'Investment in Network, Facilities, and Equipment by Content and Application Providers' (September 2014), <http://www.analysysmason.com/Research/Content/Reports/Content-application-provider-Internet-infrastructure-Sept2014/Report/> accessed 30 November 2017, fn18.
[35] Opinion 7/2000 of the Article 29 Working Party concerning the processing of personal data and the protection of privacy in the electronic communications sector (12 July 2000) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp36_en.pdf> accessed 30 November 2017, p5.
[36] Analysis Mason, (n34), p18-19.
[37] Home Office, 'Retention of Communications Data Under Part 11: Anti-terrorism, Crime and Security Act 2001, Voluntary Code of Practice' <http://www.opsi.gov.uk/si/si2003/draft/5b.pdf> accessed 30 November 2017, para 12.
[38] Section 10 of the Interception of Communications Act 1985.

otherwise stated) voice telephony, data and internet.[39] It would have been preferable for Ofcom to make a distinction between ECS and networks when giving examples of both as different legal rules may apply to each. Section 32(1) of the CA 2003 defines an ECN as a transmission system (plus associated equipment, software and stored data) for the conveyance, by the use of electrical, magnetic or electro-magnetic energy, of signals of any description i.e. a public electronic communications network includes a network of mobile phone cables or a mobile phone network[40] and the internet.[41] Section 32(2) notes that an ECS is a service consisting in, or having as its principal feature, the conveyance by means of an electronic communications network of signals, except in so far as it is a content service. The Information Commissioner's Office took this to mean that members of the public can sign up to in order to send or receive electronic signals e.g. a phone contract or internet connection,[42] thus putting ISPs within the ambit of public ECS.[43] One thing to note here however is that ISS which are not wholly involved in the conveyance of signals are not explicitly excluded from the definition of ECS. The CA 2003 implements[44] Directive 2002/21/EC (the Framework Directive),[45] and almost replicates the Article 2(a) definition of ECN. This further supports the notion that the internet is an ECN which is similar to the notion of a telecommunications system.

d. The UK's ever-expanding definitional approach, indicative of a trend?

Watson and Ingram[46] refer to the 'Twitter Joke Trial'[47] (concerning sending messages of a "menacing character" contrary to s.127(1)(a) and (3) of the CA 2003) and noted that by the High Court regarding the Internet as a public ECN (for the purposes of the CA 2003), it would put services like Twitter, an ISS,[48] under data retention obligations, which is problematic.[49] The High Court was right to agree that without the Internet, Twitter would not exist[50] but erred when it considered that a 'tweet' was a 'message' sent by a public ECS for the purposes of s.127(1).[51] Section 127(1) requires the message be sent via a public *ECN* not service. When Twitter was regarded as within the ambit of s.127(1)[52] it was unclear whether this meant a public ECN or within the definition of ECS because adding '*by* an [ECS]' implies Twitter is such a service. If it is the former (which Informm and others[53] believed), this contradicts

[39] Ofcom General Conditions Guidance <http://stakeholders.ofcom.org.uk/telecoms/ga-scheme/general-conditions/general-conditions-guidelines/> accessed 1 December 2017.
[40] Information Commissioner's Office, 'Key concepts and definitions' <https://ico.org.uk/for-organisations/guide-to-pecr/key-concepts-and-definitions/> accessed 1 December 2017.
[41] Graham Smith, (n17), 977.
[42] Information Commissioner's Office, (n40).
[43] Recital 10 of Directive 2002/21/EC; Opinion 7/2000 of the Article 29 Working Party, (n35), p5.
[44] New EC Regulatory Framework for the regulation of electronic communications, <http://www.ofcom.org.uk/static/archive/oftel/ind_info/eu_directives/> accessed 20/08/2014.
[45] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) <http://www.ofcom.org.uk/static/archive/oftel/ind_info/eu_directives/> accessed 20/08/2014.
[46] Chris Watson and Bailey Ingram, 'The Twitter Joke Judgment: The Law with Unintended Consequences?' (17 August 2012) <http://www.scl.org/site.aspx?i=ed27370> accessed 1 December 2017.
[47] *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin).
[48] Lilian Edwards, 'Section 127 of the Communications Act 2003: Threat or Menace?' (10 September 2012) <https://www.scl.org/articles/2579-section-127-of-the-communications-act-2003-threat-or-menace> accessed 1 December 2017.
[49] ibid.
[50] *Chambers*, (n47), [23-24].
[51] ibid, [25].
[52] ibid.
[53] Carrefax, 'Twitter Joke Trial | WLR (D) Case Summary' (1 August 2012) <https://carrefax.wordpress.com/2012/08/01/twitter-joke-trial-wlr-d-case-summary/> accessed 1 December

explanatory notes for the CA 2003.[54]Watson and Ingram also continued that this was indicative of a trend given the draft Communications Data Bill (dCDB) dispensed the public private network distinction altogether.[55]

e. Data Retention Investigatory Powers Act 2014 and the telecommunications service

The now repealed Data Retention Investigatory Powers Act 2014 (DRIPA 2014) continued the indicative trend of expanding the services in which retention obligations could be imposed upon. Section 1 maintained the public element. Section 5 noted that a telecommunications service was a service that consisted in the provision of access to, and of facilities for making use of, a telecommunication system *include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system* (author's emphasis).

The Explanatory Notes[56] makes clear that the definition of "telecommunications service" includes companies who provide internet-based services, such as webmail. Simply put, the definition applies to *anything* that allows or can allow the creation, management or storage of communications across networks. This is because DRIPA 2014 does not define 'communications' which could range from sending an email, a forum post, to making a search on eBay as all require communication in some form for the task at hand to be completed.

During the passage of DRIPA 2014, the then MP Elfyn Llwyd interpreted the then Clause 5 as extraordinarily affecting services outside the UK's jurisdiction.[57]James Brokenshire MP asserted that Clause 5 was intended to clarify what was always covered by the definition of telecommunications services.[58] This is simply a falsity and untenable as the public had no way of knowing how the Home Office might have interpreted the provisions either in the minds of its officials or in its previous dealings with CSPs.[59] Moreover, the provisions of 'facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system' has been *inserted* into the new definition. Carol Harlow mentions, by implication that RIPA 2000 did not extend to web-based services as she noted that proposals to include in the next Queen's Speech extensions to RIPA's[60] ambit have been announced to cover more modern forms of communication, including internet-based email, twittering and tweeting, Blackberries, Skype, mobile phone texting, social networking sites like Facebook and even online games. Kelly Fiveash reported that one industry source told El Reg that warrants under the new law could be served on publishers who provide message

2017; Informm, 'Case Law: Chambers v DPP, "Twitter joke" case, appeal successful' (29 July 2012) <https://inforrm.wordpress.com/2012/07/29/case-law-chambers-v-dpp-twitter-joke-case-appeal-successful/> accessed 1 December 2017.

[54] Explanatory notes to the CA 2003, para 87.

[55] Chris Watson and Bailey Ingram, (n46).

[56] Explanatory notes to DRIPA 2014.

[57] HC Deb 14 July, vol 584, col 691.

[58] ibid, col 786.

[59] Graham Smith, 'From Oversight to Insight - Hidden Surveillance Law Interpretations' (9 November 2015) <http://cyberleagle.blogspot.co.uk/2015/11/from-oversight-to-insight-hidden.html> accessed 3 December 2017.

[60] Carol Harlow, 'Surveillance and the Superstate' (2 May 2012) <http://ukconstitutionallaw.org/2012/05/02/carol-harlow-surveillance-and-the-superstate/> accessed 3 December 2017; This was in reference to the dropped Draft Communications Data Bill, the idea is that if the definition already covered such services elucidated by James Brokenshire, why was there a need for the relevant part of the Bill in the first place?

boards for their readers.[61] This appears to be part of a trend by the UK government to impose obligations on social media e.g. extremist content.[62] These extensions beyond RIPA 2000[63] and the Anti-terrorism Crime and Security Act 2001 (ATCSA 2001) were also noted based on what *was not* covered i.e. nothing beyond ISP and telephone company logging.[64] This demonstrates that, contrary to the assertion of Brokenshire MP, the definition of telecommunications service had been amended and significantly extended[65] by DRIPA 2014.

An example of the implications of this extension can be demonstrated with cloud-based services. Office Online can facilitate the creation of (new Word document) communications. This document would be stored on Onedrive (a cloud-based service).[66] Draft emails could also be affected as they *can be* (or have the potential to be) *transmitted*. Not an expansion *per* se[67] but DRIPA's Code of Practice stated that CSPs may therefore include those persons who provide services where customers, guests or members of the public are provided with access to communications services e.g. WiFi, that are ancillary to the provision of another service, for example in hotels, restaurants, libraries and airport lounges.[68] This obligation could be imposed on either the ISP or the ancillary service provider[69] or both, potentially creating two sets of similar or the same retained data,[70] with the latter not constituting the processing of personal data.[71] DRIPA 2014 would also catch those that are considered virtual ISPs, these are services that provide access to the internet using the infrastructure of wholesale ISPs.[72]

Another extension in DRIPA 2014, is that of an actual telecommunications operator. Section 25(1) of RIPA 2000 defined them as a person who provides a postal service or telecommunications service. Section 107(1) of the ATCSA 2001 maintained that CSPs (which could be obliged to retain) meant the same as telecommunications services in RIPA 2000. In DRIPA 2014, by virtue of s.1, a retention notice was not imposed on a CSP or public telecommunications service, but on a public telecommunications *operator*, a seemingly

---

[61] Kelly Fiveash, 'ISPs 'blindsided' by UK.gov's 'emergency' data retention and investigation powers law' *The Register* (London, 14 July 2014) <http://www.theregister.co.uk/2014/07/14/isps_blindsided_by_ukgovs_rushed_data_retention_and_investigation_powers_law/> accessed 3 December 2017.

[62] Heather Stewart, 'May calls on internet firms to remove extremist content within two hours' *The Guardian* (London, 20 September 2017) <https://www.theguardian.com/uk-news/2017/sep/19/theresa-may-will-tell-internet-firms-to-tackle-extremist-content> accessed 3 December 2017.

[63] R. Jay, 'The Data Retention and Investigatory Powers Act 2014 – Recent Developments' (15 January 2015) <https://www.scl.org/articles/3279-the-data-retention-and-investigatory-powers-act-2014-recent-developments> accessed 3 December 2017.

[64] Caspar Bowden, 'Closed circuit television for inside your head: blanket traffic data retention and the emergency anti-terrorism legislation' (2002) Duke Law and Technology Review 1 1, 5.

[65] Written evidence submitted by the Electronic Frontier Foundation (IPB0017), para 27.

[66] David Hayward, 'How to use OneDrive: A guide to Microsoft's cloud storage solution' (14 February 2016) <http://www.trustedreviews.com/how-to/how-to-use-onedrive-2945212> accessed 3 December 2017.

[67] See section 81(1) of RIPA 2000.It is noted that a telecommunication service 'facilities for making use of, any telecommunication system (*whether or not one provided by the person providing the service*).' The 'whether or not provided by the person providing the service' is akin to the ancillary purpose mentioned in the Code of Practice.

[68] Home Office, (n11), para 2.16-2.17.

[69] ibid, para 2.18.

[70] From the hotel and the ISP.

[71] Alan S. Reid, 'The European Court of Justice case of Breyer' (2017) Journal of Information Rights, Policy and Practice 2:1 1, 4.

[72] Quinton, B, 'They'll make an ISP out of you' (1999) Telephony 237:22 88; Lipof, R. 'Boardwatch' (1999) 13:12 94; Adegoke, Y, 'Eurotel to launch virtual ISP services' (2003) New Media Age 1, 9; Techopedia, 'What is a Virtual Internet Service Provider? <https://www.techopedia.com/definition/2540/virtual-internet-service-provider-visp> accessed 7 December 2015.

innocuous change. However, on deeper inspection, a public telecommunications operator by virtue of s.2(1)(a) and (b) now includes not only a provider of a public telecommunications service but *also* a person who *controls* or provides a public telecommunication *system*. There was no elaboration or clarification on what controlling a telecommunication system entails.

This applied where communications data relating to that system is either, or both, processed and stored outside the United Kingdom,[73] displaying its extra-territorial effect. The importance of this addition is that it would now catch those that fall under Smith's example, the web-hoster, as they can be argued to either control the public telecommunication system (via control of their PC) or provide it (by making it accessible to the public) and content and application providers such as Google, Facebook (whom is based in Ireland) etc,[74] thus extending the definition to individuals or companies using computers for such purposes. This may even include those who have open WiFi in their place of residence which makes it possible for members of the public to use. The inclusion of public telecommunication system controllers/providers only serves to highlight that the logical explanation would be that this definition captures not only internet based services, but also phones and particularly smart phones, and the apps that are used on them.[75]

A possible explanation for this comes from a report by Rory Cellan-Jones, where he noted that 'the security services may be more interested in targeting the likes of Google than your ISP if they want to know who you're talking to.'[76]

Cellan-Jones believed that both Google and the mobile networks already collect a significant amount of data which might be of interest to the police and intelligence services.[77] This could also be applied to web-based services.

DRIPA 2014 had been deliberately crafted with the intention to avoid doubt[78] about whether the internet and services provided over the internet can be caught by it. This would be a clear extension on who could obligate to retain, beyond that of EU law. This, technologically broadened definition, which potentially has a wide ambit[79] would not, however, be the end of it.

f. The Investigatory Powers Act 2016: A further extension

1. Extending beyond DRIPA 2014

The IPA 2016 (replacing DRIPA 2014), like the draft form sought to, amongst other things, to bring communications data retention within a single, clear piece of legislation.[80] Under the IPA 2016, the retention notices are provided for by s.87 which notes that the Secretary of State may impose, (subject to Judicial Commissioner approval)[81] a retention notice on a

[73] Home Office, (n11), para 1.5.
[74] See above.
[75] More on smart technology will be discussed when considering the Internet of Things.
[76] Rory Cellan-Jones, 'Web surveillance - who's got your data?' *BBC News* (London, 2 April 2002) <http://www.bbc.co.uk/news/technology-17586605> accessed 4 December 2017.
[77] ibid.
[78] Explanatory Notes to DRIPA 2014, para 7.
[79] Graham Smith, 'Mandatory communications data retention lives on in the UK - or does it?' (21 August 2014) <http://uk.practicallaw.com/8-577-6488> accessed 4 December 2017.
[80] Home Office, *Draft Investigatory Powers Bill* (Cm 9152 2015) para 26.
[81] Section 89 of the IPA 2016.

telecommunications operator. The major difference between IPA 2016 and DRIPA 2014 is the omission of 'public' in telecommunications operators, which would therefore apply to hosted services offering communications to businesses, or those running cloud-based communications services on behalf of businesses.[82] It would also mean that even if the web-hoster in Smith's example did not make mp3s/photos accessible to the public they could still be put under an obligation to retain. Smith himself notes that '[a] home router or domestic WiFi setup, a network within an office, school or university, or a private network of any sort would all be caught.'[83] According to Smith, this demonstrates 'a significant change from existing legislation' in which the Home Office 'has made no attempt to justify the extension to all private networks.'[84] This also highlights that the government has gradually reintroducing by stealth, the wide-reaching application of the failed dCDB.[85]

Section 261 contains definitions relevant to telecommunications, with s.261(10) noting similarly to s.2(1)(a) and (b) of DRIPA 2014 a telecommunications operator offers or provides a telecommunication service to persons in the UK or controls or provides a telecommunication systems which is wholly or partly in or controlled from the UK. The fact that a telecommunications services is offered to the person in the UK highlights the extra-territorial application of IPA 2016, as it's not the location of the service that is important, but to whom the service is offered to. This can be illustrated by Northern Ireland Court of Appeal (NICoA) in *CG v Facebook Ireland Ltd & McCloskey*.[86] Although the case concerned the e-Commerce Directive, the way in which the NICoA determined whether Facebook provided services to those in the UK is of importance. Facebook had argued that the mere fact that its services were accessible did not mean that it was established there, and therefore, could not be a data controller for the purposes of s.5 of the Data Protection Act 1998.[87] Facebook maintained that it was established in Ireland, and therefore it was Irish data protection law which had applied to them.[88] However, the NICoA disagreed holding that evidence indicates that Facebook (UK) Ltd was established for the sole purpose of making it more profitable. The NICoA continued that it conducts its activities within the UK, is responsible for engaging those within the UK who seek to use Facebook services for advertising. In addition to this, the NICoA maintained that it holds relevant data which it processes on behalf of Facebook, and even though there was no direct evidence of its connection with Facebook, there is an irresistible inference that 'in the absence of any further explanation that Facebook (UK) Ltd was established to service Facebook and is part of the wider Facebook group of companies.'[89] The NICoA was therefore, satisfied that Facebook (UK) Ltd engaged in the real and effective exercise of activity:

> [T]hrough stable arrangements in the United Kingdom and having regard to the importance of those activities to Facebook's economic enterprise the processing of data by Facebook was carried out in the context of the activities of that establishment.[90]

---

[82] Neil Brown, 'A Quick Overview of the Draft Investigatory Powers Bill' (4 November 2015) <http://www.scl.org/site.aspx?i=ed44789> accessed 4 December 2017.
[83] Graham Smith, 'The draft Investigatory Powers Bill - start all over again?' (16 February 2016) <http://www.cyberleagle.com/2016/02/the-draft-investigatory-powers-bill.html> accessed 4 December 2017.
[84] ibid.
[85] Clause 1, and 28 of the Draft Communications Data Bill.
[86] *CG v Facebook Ireland Ltd & McCloskey* [2016] NICA 54.
[87] ibid, [87].
[88] ibid, [88].
[89] ibid, [90].
[90] ibid, [91].

This establishes that even providing ancillary services to those in the UK, this could attract the application of UK law, similar to the effects doctrine under EU law.[91]

The definition of a telecommunication service[92] is a near replica of that stipulated to in s.5 of DRIPA. There are two differences, first, a telecommunication service is (if it ever was) not dependent on whether the person who provides the service also provides a telecommunication system. Second, another important point requires attention, not within the definition itself, but of terminology within the definition, that of 'communications.' Its singular is defined in s.261(2)(a) as anything comprising speech, music, sounds, visual images or data of any description, and s.261(2)(b), signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus. This confirmed the presumption highlighted earlier about communications having a wide-ranging meaning which would cover essentially any website. This is also true as this definition was inserted into DRIPA 2014 a year after it came into force via s.21(4)(a) of the CTSA 2015.[93] This is also a replica of s.81(1) of RIPA 2000, but the difference here is that 'communication' was not relevant to data retention as the word was not present in the old definition of telecommunication service (only telecommunication *system*) as it now in the IPA 2016.

2. Difficulty with defining 'communications'

The terminology of s.261(2)(b) is not straightforward in terms of its meaning. It stipulates that a communication also entails signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus. There is no indication of what a signal actually means under this subsection, is it electrical signals? If this is the case, why is this not indicated with clear terminology as such when describing telecommunication system?[94] Would hand gestures constitute impartation of anything *between* persons? If this is the case, how could it be suggested to be terminology relevant to telecommunications if telecommunications are not necessarily required for the specified act?[95] Would it be hand gestures that are carried out whilst using a telecommunication service i.e. Skype video call? What is a 'thing'? Anything? Something? Nothing? It is likely a device or object (see below), but there is no clarity. What does 'for the actuation or control of any apparatus' mean? According to the Oxford English Dictionary, actuation means to make a machine or device operate.[96] According to s.263(1) 'apparatus' ranges from 'any equipment, machinery or device (whether physical or logical)[97] and any wire or cable. What does physical and logical mean in this instance?[98] What if the physical and logical components are not

[91] Case- T-102/96 *Gencor Ltd v Commissio* [1999] ECR II-0753, [74], [89-92].
[92] Section 261(11) and (12) of the IPA 2016.
[93] Investigatory Powers Bill Research Group, <https://docs.google.com/document/d/1ZiEQJaBjUjc332dQnJkm1m4EOJNnoEtHN7hw5q9kHVk/edit?pref=2&pli=1> accessed 4 December 2017, Part 9, Chapter 2.
[94] Which makes reference to electrical and electro-magnetic energy.
[95] Hand gestures can be carried out face to face and should therefore be outside the ambit as specified by the definition of telecommunication service which requires the use of a telecommunication system.
[96] Actuate, <https://en.oxforddictionaries.com/definition/actuate> accessed 11 December 2017.
[97] The 'physical or logical' is an addition to the definition of apparatus in s.81 RIPA 2000.
[98] In terms of the internet, the physical refers to the network hardware i.e. route processer cards or power supplies. Logical refers to the non-physical i.e. IP addresses, VLAN tag. Charles R. Kalmanek, Sudip Misra, Yang Richard Yang, *Guide to Reliable Internet Services and Applications* (Springer Science & Business Media 2010), 257-258. Or it could be physical or logical designs of data warehousing. See Oracle8i, 'Data Warehousing Guide'<http://docs.oracle.com/cd/A87860_01/doc/server.817/a76994/toc.htm> accessed 4 December 2017, Part II and III.

controlled by the same entity, who then is said to be in 'control'? Are they jointly in control or does control of one component take precedence over the other? There is no attempt to explain this subsection in the explanatory notes or anywhere else, instead just referenced throughout the IPA 2016 several times. One could only assume that physical and logical are meant as a substitute for software and hardware. This subsection requires important clarifications because the definition of telecommunication services relies on what 'communication' means thus enabling a determination to which services the definition of telecommunication services apply. It is only later in section 8 that s.261(2)(b) begins to make sense.

3. Difficulty in defining telecommunications operators

Danezis highlights the difficulty in determining what a telecommunications operator is. He highlights that telecommunication services in s.261(11) is intended to include those providing services over infrastructure, logical or physical, provided by others; or software and hardware provided by others.[99] Section 261(12) maintains the notion of facilitation of the creation, management or storage of communications where Danezis is troubled by the mention of 'creation' as it might be used to argue that client side applications do facilitate the creation of communications (and their storage), and therefore are a telecommunications service. This provision thus makes potential creators of software and apps telecommunication operators.[100] It is suggested here that Danezis's concern is well founded about who this may apply to if we look back to the definition of communication in s.261(2)(a) which would include speech, music, sounds, visual images or data of any description. The 'data of any description' would seemingly catch all software and apps that communicates via a telecommunication system and thus creators themselves and the software such as web browsers[101] which can now be synced with other devices,[102] Microsoft Word,[103] and apps like WhatsApp, Google Maps[104] and any software or app that uploads and downloads (such as updating) via the internet etc would be classed as telecommunication services. Updating[105] was used as opposed to other descriptions because whilst some apps transfer images etc,[106] they all transfer data via the internet and the one thing that most if not all apps have in common is that they are frequently updated. It therefore is logical to maintain that updates are a service making software and apps that require updating is one example of making a service a telecommunication service.

4. What does 'control' mean?

The issue of the meaning of the word 'control' was mentioned above. Danezis noted the subtle differences in terminology when it came to telecommunications system and service where the former uses terminology such as 'provide' and 'control' and the latter uses 'offer.'[107] It is

[99] George Danezis, 'UK Draft IP Bill: Who is a telecommunications operator?' (7 November 2015) <https://conspicuouschatter.wordpress.com/2015/11/07/uk-draft-ip-bill-who-is-a-telecommunications-operator/> accessed 5 December 2017.
[100] ibid.
[101] Ian Jacobs and Norman Walsh, 'Architecture of the World Wide Web, Volume One' (15 December 2004) <http://www.w3.org/TR/webarch/> accessed 5 December 2017.
[102] Chrome Help, 'Sync and view tabs and history across devices' <https://support.google.com/chrome/answer/2591582?hl=en-GB> accessed 5 December 2017.
[103] For a variety of reasons, such as allowing printing via WiFi, requesting help from Office.com etc.
[104] Which requires data to be transmitted to pin point your location and to direct individuals accordingly.
[105] Graham Smith, 'The UK Investigatory Powers Act 2016 – what it will mean for your business' (29 November 2016) <https://www.twobirds.com/en/news/articles/2016/uk/what-the-investigatory-powers-bill-would-mean-for-your-business> accessed 5 December 2017.
[106] WhatsApp.
[107] George Danezis, (n99).

therefore suggested here that the use of 'control' in telecommunication systems would include home area networks (HAN). These are networks that are deployed or operated within a small boundary, typically a house or small office. This enables the communication and sharing of resources i.e. the internet between computers, laptops, mobiles, tablets, fax machines, printers, scanners,[108] games consoles, home audio systems TVs etc over a network via wired or wireless means. The contention here is that whoever controls this network, mostly likely the house/office owner/occupier or subscriber to the wide area network (WAN) service would be regarded as having 'control' of the telecommunication system for the purposes of the IPA 2016 and thus the obligation to retain could theoretically also be imposed upon them. This would likely also be the case for whoever controls, wireless personal area networks (WPAN),[109] (wireless) local area networks ((W)LAN), wireless body area networks (WBAN) which 'provides a continuous health monitoring of a patient without any constraint on his/her normal daily life activities'[110] or the intranet in, for example, schools/universities.[111] This may also raise Article 6 of the ECHR self-incrimination issues as an individual could be compelled to retain data on themselves.[112]

The addition of 'offer' a telecommunications service requires some attention, as this was not present in the dCDB[113] or DRIPA 2014[114]itself which used the word 'provide.' The difference between offer and provide is that the later involves actually giving something, while the former is usually the initial step in giving something. So, the contention here is that whether software or apps are actually given they too would be classed as telecommunication services. For example, an app that has no downloads would still fall under this definition of telecommunication service even if they have not actually provided anyone with the service in question, in essence this could be software, app, web creators etc who have yet to finish a product. This idea is supported by the fact that CSPs which are subject to technical capability notices must notify the Government of new products and services in advance of their launch, to allow consideration of the necessity and proportionality of requiring a technical capability notice on the new service.[115] Although this refers to technical capability notices, it does not change the truth of the matter, in that the Government would be aware of a new service and could use this knowledge to put the creators under retention obligations.

5. Software and Hardware vendors

Danezis makes a further point on the ambiguity of whether 'telecommunication operators' apply to software and hardware vendors.[116] Danezis notes that one could argue a software vendor provides a telecommunication system if by 'system' one is to mean the software used

[108] Techopedia, 'What is a Home Area a Network?' <https://www.techopedia.com/definition/26043/home-area-network-han> accessed 30 November 2015.
[109] 'What is wireless personal area networks?' <http://www.webopedia.com/TERM/W/wireless_personal_area_network.html> accessed 1 December 2015.
[110] Rim Negraa, Imen Jemilia, Abdelfettah Belghith, 'Wireless Body Area Networks: Applications and technologies' (2016) Procedia Computer Science 83 1274.
[111] Radar, 'Investigatory Powers Act' (5 January 2017) <https://united-kingdom.taylorwessing.com/en/insights/radar-december-2016-data-protection> accessed 5 December 2017.
[112] Conrad Fischer, 'Communications Network Traffic Data: technical and legal aspects' (2010) Eindhoven: Technische Universiteit Eindhoven, 188.
[113] Clause 28.
[114] Section 2(1)(b).
[115] Equipment Interference DRAFT Code of Practice, (2016), 7.30; Privacy International, 'UK Investigatory Powers Bill will require tech companies to notify the Government of new products and services in advance of their launch' (16 April 2016) <https://www.privacyinternational.org/node/829> accessed 26 November 2016
[116] George Danezis, (n99).

to facilitate transmissions which include the 'apparatus comprised in it'[117] with software and hardware falling in the definition of apparatus.[118] Danezis believes that software and hardware vendors of general computing equipment may be considered telecommunications operators — when their kit is *used in the context of telecommunications*.[119] Danezis warns that this interpretation could include operating systems and even processor manufacturers.

An example to highlight the scope of Danezis's observation would be to consider deep packet inspection (DPI) which can be used to detect application level threats[120] (tantamount to interception[121]) for example, in next generation firewalls[122] (NGFW).[123] This is already a feature of websites[124] and companies, such Alcatel, Cisco, Ericsson, IBM, Microsoft, Nokia and Symantec began aggressively marketing DPI technology as components of *hardware* and *software* firewalls.[125] The contention here is that software and hardware vendors employing DPI technology which is used in the context telecommunications i.e. updating could also fall within this definition of telecommunications operator.

6. Applying Danezis's principles to possibilities under the IPA 2016

These operators wherever in the world,[126] could be, after consultation,[127] put under further obligations by way of Regulations to provide facilities or services of a specified description or relating to apparatus owned or operated by a relevant operator. [128] These technical capabilities notices only apply to Part 2, 3, 5 and 6, but this would incidentally be caught by obligations under Part 4**,** which could be to retain data[129] that has been DPI'd by their software/hardware, a kind of backdoor interception and subsequent retention which could later be analysed. Kieren McCarthy argues that there may not be much point in using a virtual private network (VPN) (which would be a telecommunications service) to encrypt and conceal your web activities

[117] ibid.
[118] Section 261(13) of the IPA 2016.
[119] George Danezis, (n99).
[120] Ying-Dar Lin, Kuo-Kun Tseng, Tsern-Huei Lee, Yi-Neng Lin, Chen-Chou Hung and Yuan-Cheng Lai, 'A platform-based SoC design and implementation of scalable automaton matching for deep packet inspection' (2007) Journal of Systems Architecture 53 937, 937.
[121] European Commission, 'Legal analysis of a Single Market for the Information Society (SMART 2007/0037)' (November 2009) <http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7022&> accessed 6 December 2017.
[122] '…a hardware- or software-based network security system that is able to detect and block sophisticated attacks by enforcing security policies at the application level, as well as at the port and protocol level' Margaret Rouse, 'next-generation firewall (NGFW)' *TechTarget* <http://searchsecurity.techtarget.com/definition/next-generation-firewall-NGFW> accessed 6 December 2017.
[123] Mike O. Villegas, 'Introduction to next-generation firewalls in the enterprise' *TechTarget* (February 2015) <http://searchsecurity.techtarget.com/feature/Introduction-to-next-generation-firewalls-in-the-enterprise> accessed 6 December 2017.
[124] Sophie Stalla-Bourdillon, Evangelia Papadaki and Tim Chown, 'Metadata, Traffic Data, Communications Data, Service Use Information… What Is the Difference? Does the Difference Matter? An Interdisciplinary View from the UK' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move* (Springer 2016), 449.
[125] Margaret Rouse, 'Deep packet inspection (DPI)' *TechTarget* (November 2007) <http://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPI> accessed 6 December 2017.
[126] Section 253(8) of the IPA 2016.
[127] Section 253(6) of the IPA 2016.
[128] Section 253(4).
[129] Privacy International, (n115); Natasha Lomas, 'UK surveillance bill includes powers to limit end-to-end encryption' *TechCrunch* (Bay Area, June 2016) <https://techcrunch.com/2016/07/15/uk-surveillance-bill-includes-powers-to-limit-end-to-end-encryption/> accessed 26 November 2016.

because they could be blown open by a technical capability notice.[130] Some VPNs do not log internet traffic, but if they were required to under a technical capability notice (or under the guise of generating data), then they could also subsequently be ordered to retain this data. Lack of compliance with a technical capability notice could result in civil proceedings by virtue of s.255(10).

Any telecommunication operator and by extension service, whether it be an app, software, website, webmail or creators of said services etc could be compelled to make data retention capabilities possible if it was not possible already incidentally. Section 253(5)(c) allows the removal of electronic protection to any communications data, coupled with s.253(5)(b) the telecommunication operator could be obligated to retain by way of removing electronic protection and disclose it via s.253(5)(e). This is all possible because s.253(5) leaves open the possibility of other undefined obligations as it makes note of 'among other things' which could be used as a basis for issuing retention notices under Part 4 whether the operator is in the UK or not.[131]

When one considers the application of Bluetooth, a wireless (radio waves) technology standard for exchanging data over short distances,[132] the application of the IPA 2016's extent can further be explored. Bluetooth capabilities exists in products ranging from telephones, tablets, media players, robotics systems, handheld, laptops and console gaming equipment, and some high definition headsets, modems, and watches.[133] As Danezis warned with regards to operating systems, Bluetooth is incorporated in them.[134] If enabled Bluetooth is regarded as a telecommunication system,[135] then at the very least, devices mentioned could be regarded as telecommunication services because they provide access to or facilitate the use of Bluetooth. Also, if these devices require updating then the argument that these devices provide a telecommunication service strengthens. There is another argument that Bluetooth and indeed WiFi (and other wireless technology) enabled devices would fall under telecommunication *systems* because they enable the transmission of communications via various means of electrical and electromagnetic energy, or they could be regarded as 'apparatus,' thus whichever way it is looked at, they would fall under telecommunications operator regardless. Importantly, Bluetooth connects to the IoT.[136]

6.3 The Internet of Things and the beginning of the beyond

(a) A Brief Summary of the Internet of Things

[130] Kieren McCarthy, 'UK's new Snoopers' Charter just passed an encryption backdoor law by the backdoor' *The Register* (London, 30 November 2016) accessed <http://www.theregister.co.uk/2016/11/30/investigatory_powers_act_backdoors/> 17 January 2017.
[131] Section 253(8) of the IPA 2016.
[132] Bluetooth Technology Basics, <http://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics> accessed 6 December 2017.
[133] Bluetooth devices, <http://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-devices> accessed 6 December 2017.
[134] Apple, 'Apple Introduces "Jaguar," the Next Major Release of Mac OS X' (17 July 2002) <http://www.apple.com/pr/library/2002/07/17Apple-Introduces-Jaguar-the-Next-Major-Release-of-Mac-OS-X.html > accessed 6 December 2017; Official Lunix Bluetooth stack, <http://www.bluez.org/> accessed 6 December 2017; Microsoft, 'Bluetooth Wireless Technology FAQ' (24 July 2012) <http://download.microsoft.com/download/9/c/5/9c5b2167-8017-4bae-9fde-d599bac8184a/Bth_FAQ.docx> accessed 6 December 2017.
[135] Electromagnetic energy transferal.
[136] Bluetooth Technology Basics, (n132).

Wortmann and Flüchter have maintained, it is next to impossible in the last few months to not have come across the term 'Internet of Things' (IoT).[137] But what exactly does IoT mean? Now that the terminology is being used in a broad manner, there is no common definition.[138] The term dates back more than 15 years has been attributed to the work of the Auto-ID Labs at the Massachusetts Institute of Technology (MIT) on networked radio-frequency identification (RFID) infrastructures.[139] This term had been applied in various contexts[140] but can be summarised as 'inanimate objects that surround human beings constantly monitor, track and react to changes occurring in the local environs'[141] such as books, cars, electrical appliances and food.[142] Mattern and Floerkemeier point out that from a technical point of view, the IoT works by way of several complementary technical developments which taken together provide capabilities that help to bridge the gap between the virtual and physical world.[143] These capabilities include:

Communication and cooperation	Objects have the ability to network with Internet resources or even with each other, to make use of data and services and update their state. Wireless technologies such as GSM and UMTS, Wi-Fi, Bluetooth, ZigBee and various other wireless networking standards currently under development, particularly those relating to Wireless Personal Area Networks (WPANs).
Addressability	Within an Internet of Things, objects can be located and addressed via discovery, look-up or name services, and hence remotely interrogated or configured.
Identification	Objects are uniquely identifiable. RFID, NFC (Near Field Communication) and optically readable bar codes are examples of technologies with which even passive objects which do not have built-in energy resources can be identified (with the aid of a "mediator" such as an RFID reader or mobile phone). Identification enables objects to be linked to information associated with the particular object and that can be retrieved

[137] Felix Wortmann, and Kristina Flüchter, 'Internet of Things - Technology and Value Added' (2015) Business & Information Systems Engineering 57:3 221, 221.
[138] ibid.
[139] ibid; Luigi Atzori, Antonio Iera and Giacomo Morabito, 'The Internet of Things: A survey' (2010) Computer Networks 54:15 2787, 2788; Friedemann Mattern and Christian Floerkemeier, 'From the internet of computers to the internet of things' in Kai Sachs, Ilia Petrov and Pablo Guerrero (eds) *From Active Data Management to Event-Based Systems and More* (Springer, Berlin, Heidelberg 2010), 243.
[140] Friedemann Mattern and Christian Floerkemeier, (n139).
[141] Alan S. Reid, 'Is society smart enough to deal with smart cards?' (2007) Computer Law Security Report 23:1 53, 54.
[142] Commission, 'Internet of Things – An action plan for Europe' (Communication) COM/2009/0278 final.
[143] Friedemann Mattern and Christian Floerkemeier, (n139).

	from a server, provided the mediator is connected to the network.
Sensing	Objects collect information about their surroundings with sensors, record it, forward it or react directly to it.
Actuation	Objects contain actuators to manipulate their environment (for example by converting electrical signals into mechanical movement). Such actuators can be used to remotely control real-world processes via the Internet.
Embedded information processing	Smart objects feature a processor or microcontroller, plus storage capacity. These resources can be used, for example, to process and interpret sensor information, or to give products a "memory" of how they have been used.
Localization	Smart things are aware of their physical location, or can be located. GPS or the mobile phone network are suitable technologies to achieve this, as well as ultrasound time measurements, UWB (Ultra-Wide Band), radio beacons (e.g. neighbouring WLAN base stations or RFID readers with known coordinates) and optical technologies.
User interfaces	Smart objects can communicate with people in an appropriate manner (either directly or indirectly, for example via a smartphone). Innovative interaction paradigms are relevant here, such as tangible user interfaces, flexible polymer-based displays and voice, image or gesture recognition methods.

Table A

The European Commission summarises the mode of communications as: things-to-person communication and thing-to-thing communications, including Machine-to-Machine (M2M) communication.[144] Mattern and Floerkemeier describe this interaction as an individual using their smart phone, to communicate with the Thing (smart object) which then communicates with the internet, which then communicates back to the smart phone and displaying information to the individual.[145]

(b) The IoT and the IPA 2016

[144] Commission, (n142).
[145] Friedemann Mattern and Christian Floerkemeier, (n139).

The Institute for Human Rights and Business were (IHRB) concerned about the definitions of telecommunications services and systems as these definitions would encompass 'Big Data' and the IoT.[146] The IHRB felt it was unclear as to whether the definitions in the IPA 2016 would include 'devices that generate data relating to individuals that may not involve communication between two people, but instead machine-to-machine communication.'[147] It is only once a basic understanding of the IoT is gained can one properly comprehend s.261(2)(b) of the IPA 2016 that can address IHRB's concerns in the affirmative. Section 261(2)(b) indicates that 'communication' involves signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus. Section 261(2)(b) is intended to cover communications by way of the IoT, but this inclusion would mean that the machinery behind the IoT would fall under the definition of telecommunication service as it *consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system* e.g. Bluetooth enabled devices and WiFi. Furthermore, devices, objects or Things would also be caught under the definition of telecommunication system because of conveyance of signals i.e. Bluetooth including the apparatus comprised, thus the IoT and associated hardware would fall under telecommunication operator however these definitions are approached. Moreover, the obligation to retain could fall upon natural or legal persons owning IoT devices as a telecommunications operator includes one who provides or *controls* the telecommunications system. The magnitude of the implications of this inclusion cannot be overstated because such technologies are already in place to some degree such as wearable tech,[148] smart electricity meters,[149] TVs[150] future smart cities,[151] the list could continue to applications such as transportation and logistics, healthcare, personal and social settings[152] and even the home[153] in which the US director of national intelligence has admitted will occur in the future.[154] All would fall within the definition of telecommunications operator. The concern with smart objects is that they can accumulate a massive amount of data[155] which the characteristics of such traffic are currently unknown[156] could subsequently be retained, thus potentially turning our home into the least technologically private place in the IoT era. As Atzori *et al* have maintained that the ways in which data collection, mining, and provisioning will be accomplished in the IoT are completely different from current methods, providing an amazing number of occasions for personal data to be collected, thus making it impossible for

[146] Written evidence submitted by the Institute for Human Rights and Business written evidence (IPB0094), para 4.2.
[147] ibid, para 4.3.
[148] Kelsey Finch and Omer Tene, 'Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town' (2015) Fordham Urban Law Journal 41:5 1581, 1601-02.
[149] Friedemann Mattern and Christian Floerkemeier, (n139).
[150] John Ribeiro, 'Samsung faces complaint to FTC over Smart TV 'surveillance'' (26 February 2015) <http://www.infoworld.com/article/2889458/federal-regulations/samsung-faces-complaint-to-ftc-over-smart-tv-surveillance.html> accessed 8 December 2017.
[151] Felix Wortmann, and Kristina Flüchter, (n137), 222; Department for Digital, Culture, Media & Sport and Ed Vaizey, 'Manchester wins £10m prize to become world leader in 'smart city' technology' (3 December 2015) <https://www.gov.uk/government/news/manchester-wins-10m-prize-to-become-world-leader-in-smart-city-technology> accessed 8 December 2017.
[152] Luigi Atzori, Antonio Iera and Giacomo Morabito, (n139), Fig. 3.
[153] ibid.
[154] Trevor Timm, 'The government just admitted it will use smart home devices for spying' *The Guardian* (London, 9 February 2016) <https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government> accessed 8 December 2017.
[155] Friedemann Mattern and Christian Floerkemeier, (n139).
[156] Luigi Atzori, Antonio Iera and Giacomo Morabito, (n139), 2800.

individuals to control disclosure.[157] This information could be retained indefinitely and will affect individuals that do not even use any IoT service.[158] There have already been privacy concerns raised by the Global Privacy Enforcement Network Sweep (GPENS) about the IoT and how companies handle personal data.[159] The ICO made a statement highlighting the potential benefits of the IoT but that it should not be at the cost of our privacy.[160] The European Commission made the distinction between connection in restricted areas (intranet of things) as opposed to the IoT which they regard as publicly accessible,[161] DRIPA 2014 only applied the public element whereas the IPA 2016 makes no such distinction. Given the concerns highlighted above, it is appropriate to consider the 'family life' and 'home' aspects of Article 8.

(c) *Home and Family Life in the IoT*

1. Home

In *Klass* the ECtHR did not rule out that secret surveillance could interfere with a person's home.[162] The ECtHR noted that the living instrument doctrine (interpretation in light of societal changes and in line with present-day conditions) has allowed an extensive[163] interpretation of home. [164] In *Szabo and Vissy*[165] the ECtHR held that searching and surveillance 'to monitor their electronic communications and computer data transmissions and to make recordings of any data acquired through these methods' interfered not only with private life and correspondence, but also the home. Home would be interfered with even if this was not a seizure imposed in criminal proceedings.[166]

The IoT brings hidden risks into the home,[167] such as the ease 'for a passive network observer to infer user behavior from encrypted smart home traffic'[168] from metadata (IP packet headers, TCP packet headers, and send/receive rates)[169] *without* the use of DPI.[170] Such network observers include ISPs (a telecommunications operator), Wi-Fi eavesdroppers, or state-level

[157] ibid, 2802.
[158] ibid.
[159] 'Results of the 2016 Global Privacy Enforcement Network Sweep' (22 September 2016) <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/bg_160922/> accessed 22 September 2016.
[160] ICO News, 'Privacy regulators study finds Internet of Things shortfalls' (22 September 2016) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/09/privacy-regulators-study-finds-internet-of-things-shortfalls/> accessed 22 September 2016.
[161] Commission, 'Internet of Things – An action plan for Europe' COM(2009) 278.
[162] *Klass v Germany* App no. 5029/71 (ECHR, 6 September 1978, [41].
[163] Ivana Roagna, 'Protecting the right to respect for private and family life under the European Convention on Human Rights' (2012) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806f1554> accessed 6 April 2017, p30-32.
[164] *Demades v Turkey* App no. 16219/90 (ECHR, 31 July 2003), [33].
[165] *Szabo and Vissy v Hungary* App no. 37138/14 (ECHR, 12 January 2016), [52].
[166] *Bernh Larsen Holding AS and Others v. Norway* App no. 24117/08 (ECHR, 14 March 2013), [106].
[167] BITDEFENDER, 'The hidden risks of bringing the Internet of Things into your home' (10 December 2015) <http://mashable.com/2015/12/10/iot-home-security-brandspeak/#z4F6Xk4zrsqF> accessed 8 December 2017.
[168] Noah Apthorpe, Dillon Reisman and Nick Feamster, 'A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic' (2016) <https://arxiv.org/pdf/1705.06805.pdf> accessed 8 December 2017, p4.
[169] ibid, p2.
[170] ibid, p4.

surveillance entities[171] and such behaviour included sleep patterns, when appliances were used, when a camera feed was monitored and when it detects motion,[172] or Amazon's Alexa which can detect and ignore even in sleep mode.[173] It has also been demonstrated that medical IoT devices can reveal 'cleartext information that may reveal sensitive medical conditions and behaviours.'[174] If this trend continues, Silkie Carlo of Big Brother Watch argues we will become 'society of watched consumers subjected to the most granular, pervasive and inescapable surveillance. It is a terrifying thought.'[175]

2. *Family Life, the Home and Smart Meters*

Baroness Hale in *Countryside Alliance* highlighted the separate but related fundamental values of 'the inviolability of the home and personal communications from official snooping.'[176] Smart metering is used as an example to demonstrate this. Smart metering can be described as:

> [A] new generation of advanced and intelligent metering devices which have the ability to record the energy consumption of a particular measuring point in intervals of fifteen minutes or even less…[that] can also communicate and transfer the information recorded in real time or at least on a daily basis by means of any communications network to the *utility company* for purposes such as monitoring of the system load as well as for billing purposes (author's emphasis).'[177]

The utility company could be a telecommunications service because it consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted. It may also be a telecommunications system because providing the smart meter includes the conveyance of signals and the apparatus comprised. Thus, the utility company would be a telecommunications operator for providing an ancillary service.

Smart meters can give insights into patterns of living.[178] It can determine when a person is at home, sleeping, when they are preparing meals and the type (hot or cold), what appliances are used, when the kids are at home and even the channel the TV is tuned into.[179] It can even be

---

[171] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan and Nick Feamster, 'Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic' (2017) <https://arxiv.org/pdf/1708.05044.pdf> accessed 8 December 2017, p2.
[172] ibid.
[173] Tekla S. Perry, 'A Sleeping Alexa Can Listen for More Than Just Her Name' (9 February 2018) <https://spectrum.ieee.org/view-from-the-valley/consumer-electronics/gadgets/beyond-the-super-bowl-a-sleeping-alexa-can-listen-for-more-than-just-her-name.amp.html?__twitter_impression=true> accessed 17 June 2018.
[174] Daniel Wood, Noah Apthorpe and Nick Feamster, 'Cleartext Data Transmissions in Consumer IoT Medical Devices' (2017) IoT S&P'17 7.
[175] Alex Hern, 'UK homes vulnerable to 'staggering' level of corporate surveillance' *The Guardian* (London, 1 June 2018) <https://www.theguardian.com/technology/2018/jun/01/uk-homes-vulnerable-to-staggering-level-of-corporate-surveillance> accessed 17 June 2018.
[176] *Countryside Alliance and others, R (on the application of) v Attorney General & Anor* [2007] UKHL 52, [116].
[177] Rainer Knyrim and Gerald Trieb, 'Smart metering under EU data protection law' (2011) International Data Privacy Law 1:2, 121.
[178] Colette Cuijpers and Bert-Jaap Koops, 'Smart Metering and Privacy in Europe: Lessons from the Dutch Case' in Serge Gutwirth, Ronald Leenes, Paul de Hert, Yves Poulle (eds) *European Data Protection: Coming of Age* (Springer 2013), 277; Andres Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin, 'Private Memoirs of a Smart Meter' (2010) <http://lass.cs.umass.edu/papers/pdf/buildsys10.pdf> accessed 9 December 2017.
[179] Colette Cuijpers and Bert-Jaap Koops, (n178), 285.

utilised to inform health care professionals.[180] This was argued to constitute a breach of the inviolability of the home and right to family life because smart meter usage does not just concern informational privacy, but also the effects the generation of that data has on spatial and relational privacy.[181] Cuijpers and Koops asked the important questions of how smart meters could induce a chilling effect in the home and thus also interfere with family life:

> Are the occupants hindered in their right to an uninhibited home life? Do the occupants feel free to enter into relationships? It is by no means unthinkable that some occupants might feel embarrassed by the knowledge that their grid manager is 'watching' behind the front door and, for example, might be able to deduce from the meter readings that, with an otherwise 'average' energy-consumption pattern, the occupant regularly comes home between the hours of 2 and 3 a.m. on Friday nights and consumes more energy the next morning than on other days. Does this mean that two people are showering in this single-person household?[182]

This has demonstrated that whether the telecommunications operator is the ISP or the provider of the IoT device, how family life and home can and will be interfered with. The smart meter was just one example of how our homes are becoming more transparent.[183]

6.4 The Obligation to retain extends beyond the Secretary of State and Judicial Commissioners

(a) Who else can obligate Data Retention?

Under s.61(1) of the IPA 2016, a designated senior officer (DSO) of a relevant public authority can obtain communications data for specific investigations/operations or for testing, developing or maintaining ways relating to the availability or obtaining communications data. A DSO is defined in s.70(3) of the IPA 2016, as a person holding office, rank or position in relation to the authority i.e. Superintendent of a police force.[184]

(b) DSO Authorisations

Section 61(2) allows the DSO authority to engage in conduct which is for the purpose of obtaining the data from any person which relates to a telecommunication system, or data derived from a telecommunication system. It is unclear whether data in this section is interchangeable with communications data. As noted above, data is far broader in scope than communications data, and if the former is used, this increases the severity of interference with fundamental rights.

Section 61(4)(c)(i) allows an authorised officer to where they believe a telecommunications operator is *not already in* possession of but *maybe or is capable of obtaining any*

---

[180] Louise Rogerson, 'How a smart meter could save your life' *The Spectator* (18 July 2018) <https://health.spectator.co.uk/how-a-smart-meter-could-save-your-life/?_lrsc=dbc7fdf0-368e-4711-9bae-da8fa3fa3d4b&_lrsc=cf7b4f02-2490-43e2-98c6-d075e421c98c> accessed 30 July 2018.
[181] Colette Cuijpers and Bert-Jaap Koops, 'The 'smart meters' bill: a privacy test based on article 8 of the ECHR' (2008) <https://skyvisionsolutions.files.wordpress.com/2014/11/dutch-smart-meters-report-tilt-october-2008-english-version.pdf> accessed 9 December 2017, p21.
[182] ibid.
[183] Colette Cuijpers and Bert-Jaap Koops, (n178), 293.
[184] Schedule 4 Part 1 of the IPA 2016.

communications data (author's emphasis), by notice, require them to obtain data that is not already in their possession and disclose data subsequently obtained by them. Moreover, s.61(5)(a) allows authorisations for data that did not exist at the time of the authorisation. This could require telecommunications operators to generate and *retain* they may normally would not. The explanatory notes for the IPA 2016 maintains that s.61(5)(a) allows a relevant public authority to request communications data on a forward-looking basis in respect of a known subject of interests.[185] This also implies that if data is not already in existence, the telecommunications operator in question has *not* been served with a retention notice. Section 61(5)(b) allows for the authorisation of obtaining or disclosure of data by those who are not authorised officers for the enabling of obtaining communications data. Section 61(5)(b) does not indicate who would fall into the category of 'not an authorised officer' and therefore leaves the DSO with wide discretion on who that may be in any instance. Could this be an officer who do not have authorisation within the relevant public authority? Or could it be anyone (as s.61(5)(b) refers to 'person') who the DSO chooses? An indicator of the definition of person can be found under s.81(1) of RIPA 2000 as including any organisation and any association or combination of persons. Therefore, the possible obligations to generate or retain data could be imposed on a very broad category of persons. Section 61(5)(c) indicates that an authorisation can require a telecommunications operator who controls or provides a telecommunication system to obtain or disclose data relating to the use of a telecommunications service provided by another telecommunications operator, therefore requiring third-party interception. Due to the references to 'data' rather than 'communications data,' this potentially widens the scope of what data a telecommunications operator could obtain from third parties (given that s.86(3) refers to *general definitions*). In order to quell this inconsistency, it would be advisable to add to s.86(1) that 'in this Part any reference to 'data' means communications data within the meaning of s.261(5).' This is also possible through the purposive interpretation of s.3(1) of the Human Rights Act 1998 (HRA 1998) (which has been linked to the EU principle of indirect effect)[186] which provides that 'so far as it is possible to do so' all legislation 'must be read and given effect in a manner which is compatible with the' ECHR.[187] The White Paper of the HRA 1998, acknowledged that s.3 was to go 'far beyond the present rule which enables the courts to take the Convention into account in resolving any *ambiguity* in a legislative provision (author's emphasis).'[188] One way of doing so, as the majority of the UK House of Lords endorsed is to 'read in words which change the meaning of the enacted legislation, so as to make it Convention-compliant.'[189] Another way is to interpret data restrictively[190] as *only* meaning communications data. Any of the approaches identified would ensure that any powers, if used to retain communications data, are not just as broad, or broader than the powers provided by retention notices, which could ultimately defeat the purpose of that provision. It would also serve to prevent hidden interpretations.[191]

(c) Who can be obligated to retain by Public Authorities?

Section 86(3) of the IPA 2016 when referring to telecommunications definition indicating the definition of telecommunications operator applies, thus highlighting that public authorities can

[185] Explanatory Notes of the IPA 2016, para 177.
[186] Abigail Schaeffer, 'Linking Marleasing and s. 3(1) of the Human Rights Act 1998' (2005) Judicial Review 10:1 72.
[187] Jan van Zyl Smit, 'The New Purposive Interpretation of Statutes: HRA Section 3 after Ghaidan v Godin-Mendoza' (2007) MLR 70:2 294, 295.
[188] Secretary of State for the Home Department, *Rights Brought Home* (White Paper, Cm 3782 (1997)), para 2.7.
[189] *Ghaidan v Godin-Mendoza* [2004] UKHL 30, [32].
[190] ibid.
[191] Graham Smith, (n59).

obligate data retention on the same services as the Secretary of State and Judicial Commissioners. The caveat is that s.61(4)(a) allows authorised officers to obtain communications data themselves or from any person or telecommunications system. There are grounds to believe this is already occurring where six police forces in the UK have brought 'IMSI-catchers' that can both track the movements of mobile phone users within a given area, and intercept texts and calls.[192] Section 61(4)(b)(i) allows authorised officers to ask *any person* whom the authorised officer believes is, maybe or is not in possession of the communications data but is capable of obtaining it, to obtain it.' The requirement of telecommunications operator is not present and would therefore not require the telecommunications operator to do anything, so long as a person, *any* person could achieve the same objective. This creates a variety of problems, one being, would this allow the authorised officer to ask a hacker to retrieve communications data from a telecommunications operator? This highlights another issue, s.61(4)(b) does not specify where this person must obtain communications data *from*. All that is required is that this person is believed to be capable of obtaining it. Beyond the definition of telecommunications operator, public authorities may have broader powers of who they can obligate and what they can do to retain than the Secretary of State/Judicial Commissioners, nor does the communications data require the condition of relevancy.

6.5 Conclusions

This Chapter has demonstrated that the obligation to retain has expanded from ISPs, to now also include webhosts, websites, cloud based services, controllers of various networks (personal, home, local), the devices that are associated with them, to apps, software, hardware and devices falling under the IoT and essentially anything that communicates. This represents an extension beyond EU law. This Chapter also supplemented Chapter 4 in highlighting that who is obligated to retain has implications for the family life and home aspects of Article 8 given that IoT devices will be sending data about traditional home products. Chapter 5 concluded on the idea the people are more likely to feel the surveillance aspects of laws when it applies to IoT devices. One of the tasks of this Chapter is considering whether data retention would be applicable to IoT devices, and has concluded that it would, and so not only would private companies be able to spy on individuals through IoT deivces, but the UK government could compel them to keep that data for their own purposes.

When giving written evidence on the IPA 2016, Adrian Kennard, Director of ISP Andrews & Arnold Ltd maintained that '[t]he [IPA 2016] should use a consistent set of definitions such as reference to the Communications Act, and should only apply powers to public communications providers.'[193] Finally, this Chapter highlighted that the power to obligate retention is not exclusively with the Secretary of State and Judicial Commissioner, but also relevant public authorities and anyone they believe is capable of carrying out such a task. As of writing this thesis, the UK Government have opened a (now closed) consultation on changes to s.61 in terms of the purposes to obtain communications data,[194] the implications of these will be considered in Chapter 8 (Conclusions).

---

[192] Alon Aviram, 'Revealed: Bristol's police and mass mobile phone surveillance' (October 2016) <https://thebristolcable.org/2016/10/imsi/> accessed 22 October 2016.

[193] Investigatory Powers Bill Written evidence submitted by Adrian Kennard (IPB 13) (March 2016) <http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB13.htm> accessed 11 December 2017

[194] Home Office, 'Investigatory Powers Act 2016' (30 November 2017) <https://www.gov.uk/government/consultations/investigatory-powers-act-2016> accessed 11 December 2017.

Chapter 7: Data Retention is Incompatible with the ECHR

7.1 Introduction

> …the level of protection afforded by the Charter must never be inferior to that guaranteed by the ECHR.[1]

Advocate General (AG) Saugmandsgaard Øe acknowledged that the Charter of Fundamental Rights (CFR) must be at the very least, equal to the European Convention on Human Rights (ECHR or Convention Rights) in regards to the protections they offer.

This Chapter has two tasks, it first highlights the deficiencies of the Court of Justice of the European Union's (CJEU) judgments in both *Digital Rights Ireland*[2] and *Tele2 and Watson*.[3] Namely, the CJEU did not, at the very least adhere to the strict requirement of data retention measures being in 'accordance with the law,' a principle well established in the jurisprudence of the European Court of Human Rights (ECtHR). The CJEU's basis for permissible retention i.e. identifying a public, is much looser than the ECtHR's reasonable suspicion. The CJEU's acceptance of geographical data retention is also problematic from an ECHR discrimination perspective. Despite the highlighted deficiencies in the CJEU's approach, it will be highlighted that the Investigatory Powers Act 2016 (IPA 2016) does not even satisfy the requirements of *Digital Rights Ireland* or *Tele2 and Watson*.

The second task, takes a step further, in arguing that data retention found within Part 4 (mainly s.87) of the IPA 2016 does not satisfy any of the requirements of legality, necessity and proportionality found within the Convention Rights (Articles 8-11 and Article 2 Protocol 4). It will also highlight that Article 6(2) and 6(3)(c) of the ECHR is potentially violated, and all the above Convention Rights are violated in conjunction with Article 14. Such discussion will also consider data retention judgements in other EU member states,[4] the severity of interference with fundamental rights, who is obligated to retain,[5] and therefore *what* data is retainable, to supplement ECHR arguments.

The compatibility of the IPA 2016 with the ECHR undergoes the strict tests of whether the measures are 'in accordance with the law,' and 'necessary in a democratic society.' These two tests subdivide, with the former being broken down into the IPA 2016's accessibility and foreseeability. Regarding foreseeability, the case law of the ECtHR's Grand Chamber GC) has reaffirmed several minimum safeguards in the area of secret surveillance to avoid abuses of power, notably that:

1. the nature of offences which may give rise to an interception order;
2. a definition of the categories of people liable to have their telephones tapped;

---

[1] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-572, Opinion of Saugmandsgaard Øe, [141].
[2] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECR I-238.
[3] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-970.
[4] Matthew White, 'Protection by Judicial Oversight, or an Oversight in Protection?' (2017) Journal of Information Rights, Policy and Practice 2:1, 2.
[5] See Chapters 3 and 5.

3. a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained;
4. the precautions to be taken when communicating the data to other parties;
5. and the circumstances in which recordings may or must be erased or destroyed.[6]

With regards to the latter, the question becomes whether the IPA 2016 corresponds to a 'pressing social need,' whether it was 'proportionate to the legitimate aim pursued,' i.e. least restrictive measure and whether the reasons given by the national authorities to justify it are relevant and sufficient. Not only will this analysis highlight the deficiencies in the IPA 2016, but also highlight where the interpretation of the CFR is inferior to the ECHR.

7.2 Criticism of the CJEU's approach to data retention

Digital Rights Ireland has been regarded as ground-breaking,[7] a milestone,[8] a significant step in developing fundamental rights protection[9] (even in the national security context)[10] and a landmark judgment.[11] Marie-Pierre Granger and Kristina Irion noted that the ruling meant that blanket data retention was no longer possible,[12] a position agreed upon by Michael Ryan.[13] It also meant that limitations included retention being confined to situations which pose a threat to public security by restricting the measure to a time period, geographical zone or groups of persons likely to be involved in a serious crime or, more broadly, to persons whose communications data can otherwise contribute to law enforcement.[14]

The CJEU's position is regarded as closing ranks with the ECtHR jurisprudence by treating collection and use of data as two separate interferences with privacy and data protection.[15] McIntyre argues that it in fact extends protection beyond the ECtHR jurisprudence in that it relied on *ex post facto* controls and takes a step further with regards to need for prior judicial control.[16] However, it has also been argued that this merely reflects already (but not often cited)

---

[6] *Roman Zakharov v Russia* App no. 47143/06 (ECHR, 4 December 2015), [231].
[7] Emily Barabas, 'European Court of Justice: EU Data Retention Directive Infringes on Human Rights' (April 10 2014) <https://cdt.org/blog/european-court-of-justice-eu-data-retention-directive-infringes-on-human-rights/> accessed 12 June 2017.
[8] Federico Fabbrini, 'Human Rights in the Digital Age The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.' (2015) Harvard Human Rights Journal 28 65, 67.
[9] Judith Rauhofer and Daithí Mac Síthigh, 'The Data Retention Directive Never Existed' (2014) SCRIPTed 11:1 118; EDPS, 'Press Statement: The CJEU rules that Data Retention Directive is invalid' (8 April 2014) <https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2014-08_press_statement_drd_en.pdf> accessed 12 June 2017.
[10] Federico Fabbrini, (n8), 84.
[11] Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) European Law Review 6 835, 844; Nora Ni Loideain, 'EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era' (2015) Media and Communication 3:2 53, 54.
[12] Marie-Pierre Granger and Kristina Irion, (n11), 848.
[13] Michael. H. Ryan, 'Is government access to your communications data lawful? The decision of the Divisional Court in Davis v Home Secretary' U.L.R. [2015] 20:5, 55-60.
[14] Marie-Pierre Granger and Kristina Irion, (n11), 848.
[15] ibid, 847.
[16] T.J. McIntyre, 'Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective' in Martin Scheinin, Helle Krunke, and Marina Aksenova (eds) *Judges as Guardians of Constitutionalism and Human Rights* (Edward Elgar 2015).

existing ECtHR jurisprudence.[17] It has also been regarded as putting an end to mass surveillance and comes to the same conclusion as AG Cruz Villalón, but for different reasons.[18]

Initial reactions to the CJEU's judgment in *Tele2 and Watson* were positive, many regarding it as a blow to the UK data retention surveillance regime.[19] The Legal Services of the Council of the EU acknowledged that 'a general and indiscriminate retention obligation for crime prevention and other security reasons would no more be possible at national level than it is at EU level.'[20]

a. Were all the criticisms in Digital Rights Ireland mandatory requirements?

One of the issues for disagreement between the English and Welsh High Court (HC) and Court of Appeal (CoA)[21] was whether the criticisms of *Digital Rights Ireland* were mandatory requirements. AG Saugmandsgaard Øe believed that they were,[22] whereas the CJEU did not hold that the safeguards mentioned in *Digital Rights Ireland* were mandatory requirements, but cited it approvingly.[23] This raises the question whether the requirements were mandatory at all. For Open Rights Group (ORG), particularly prior judicial/independent authorisation was enough to signal a blow to the current self-authorisation system in the UK,[24] which the UK Government, in any event is seeking to comply with (in terms of authorisation),[25] and the CoA[26] partially[27] ruled consistently with.

---

[17] Matthew White, (n4), 5-6.
[18] Steve Peers, 'The data retention judgment: The CJEU prohibits mass surveillance' (8 April 2014) <https://eulawanalysis.blogspot.co.uk/2014/04/the-data-retention-judgment-cjeu.html> accessed 13 June 2017.
[19] Javier Ruiz, 'EU Court slams UK data retention surveillance regime' (21 December 2016) <https://www.openrightsgroup.org/blog/2016/eu-court-slams-uk-data-retention-surveillance-regime> accessed 21 June 2017; Julia Fioretti, 'EU court says mass data retention illegal' (21 December 2016) <http://uk.reuters.com/article/uk-eu-court-privacy-idUKKBN14A0YD> accessed 21 June 2017; Owen Bowcott, 'EU's highest court delivers blow to UK snooper's charter' *The Guardian* (London, 21 December 2016) <https://www.theguardian.com/law/2016/dec/21/eus-highest-court-delivers-blow-to-uk-snoopers-charter> accessed 21 June 2017; Nicole Kobe, 'Blow for Snoopers Charter as EU court bans mass data collection' *ITPro* (21 December 2016) <http://www.itpro.co.uk/public-sector/snoopers-charter/27819/blow-for-snoopers-charter-as-eu-court-bans-mass-data-collection> accessed 21 June 2017; Liberty, 'Government IS breaking the law by collecting everyone's internet and call data and accessing it with no independent sign-off and no suspicion of serious crime' (21 December 2016) <https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/government-breaking-law-collecting-everyones-internet-and-call> accessed 21 June 2017.
[20] Legal Services letter to Permanent Representatives Committee, Brussels, 1 February 2017 (OR. en) 5884/17, para 14; see also Anna Biselli, 'EU discusses future of data retention: "Indiscriminate retention no longer possible"' (31 May 2017) <https://edri.org/eu-discusses-future-of-data-retention-indiscriminate-retention-no-longer-possible/> accessed 22 June 2017.
[21] See Chapter 2.
[22] Opinion of Saugmandsgaard Øe, (n1), [221].
[23] Lorna Woods, 'Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)' (21 December 2016) <https://eulawanalysis.blogspot.co.uk/2016/12/data-retention-and-national-law-ecj.html> accessed 21 June 2017.
[24] Javier Ruiz, (n19).
[25] Alexander J Martin, 'Home Office admits it's preparing to accept EU ruling on surveillance' *The Register* (London, 21 March 2017) <https://www.theregister.co.uk/AMP/2017/03/21/home_office_admits_its_preparing_to_accept_eu_ruling_on_surveillance/> accessed 21 June 2017; Home Office, 'Investigatory Powers Act 2016' (30 November 2017) <https://www.gov.uk/government/consultations/investigatory-powers-act-2016> accessed 16 February 2018.
[26] *Tom Watson and Others v Secretary of State for the Home Department* [2018] EWCA Civ 70.
[27] Matthew White, 'Data Retention is still here to stay, for now…' (5 February 2018) <https://eulawanalysis.blogspot.co.uk/2018/02/data-retention-is-still-here-to-stay.html> accessed 16 February 2018.

b. In accordance with the law

The legal requirement for measures that interfere with qualified fundamental rights, under the ECHR must be what is described as being 'in accordance with the law.'[28] In *Digital Rights Ireland*, the CJEU skipped this requirement entirely[29] where Ojanen noted that the 'absence of the explicit application of the 'quality of the law' requirement is all the more striking' as AG Cruz Villalón considered this in great detail.[30]

In *Tele2 and Watson* AG Saugmandsgaard Øe invited the CJEU to confirm that 'in accordance with the law' under the ECHR meant the same thing for data retention.[31] He noted that the ECHR requirement[32] and that 'provided by law' in Article 52(1) CFR *needs* to be the same as the ECHR for the following reasons (author's emphasis):[33]

i. The level of protection provided by CFR 'must *never* be inferior to that guaranteed by the ECHR' and '*must be at least as stringent* as that given to it by the [ECtHR] in connection with the ECHR;' (author's emphasis) and
ii. It would be inappropriate to impose different criteria on Member States 'depending on which of those two instruments was under consideration.'[34]

Therefore, AG Saugmandsgaard Øe felt that 'retention obligations…*must* be founded on a legal basis that is adequately accessible and foreseeable and provides adequate protection against arbitrary interference' (author's emphasis).[35] This would also prevent the CJEU falling into 'the trap of tautologically regarding a legal norm, the validity of which is being questioned, as being allegedly in accordance with the law because it is a law.'[36] The CJEU, however, did not address AG Saugmandsgaard Øe's invitation and thus leaves a deficiency in the protection of fundamental rights (see section 7.4 below).

c. Essence of the Right

The CJEU has consistently held that although interference posed by data retention is particularly serious, this did not affect the essence of Article 7 because content of communications was not retained.[37] However, as was argued in Chapter 3, this line of reasoning is unsustainable whether retention was under Directive 2006/24 (the Data Retention Directive (DRD)) or Part 4 of the IPA 2016, as such measures affect the very substance of the right, and the essence of the right.[38]

[28] See section 7.3 below.
[29] Marie-Pierre Granger and Kristina Irion, (n11), 842.
[30] Tuomas Ojanen, 'Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance' (2014) European Constitutional Law Review 10: 528, 536.
[31] Opinion of Saugmandsgaard Øe, (n1), [137].
[32] ibid, [138-9].
[33] ibid, [140].
[34] ibid, [141-2].
[35] ibid, [143].
[36] Gloria González Fuster, 'Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection' (2014) Birkbeck Law Review 2:2 263, 271.
[37] *Digital Rights Ireland and Seitlinger and Other*s, (n2), [39]; *Tele2 Sverige AB and Watson*, (n3), [101].
[38] Marie-Pierre Granger and Kristina Irion, (n11), p847.

The CJEU also acknowledged, just as AG Saugmandsgaard Øe had, that communications data is no less sensitive than the actual content of communications,[39] but *still* refused to suggest this would adversely affect the essence of the right.[40] This appears paradoxical given that the CJEU agreed with AG Saugmandsgaard Øe that 'that data retention *creates an equally serious interference with rights as measures which intercept the content*' and 'that the risks associated with the access to communications *maybe greater* than access to the content of communications (author's emphasis)**.**'[41] This is also now in contrast with the position of the ECtHR in *Big Brother Watch* (see Chapter 3) in which they were not persuaded that content is more intrusive than communications data. This is because as Chapter 3 (with many more examples) noted, communications data is highly intrusive, structured, making it more suitable for aggregation and analysis. Furthermore, content can be disguised more easily through encryption[42] or using coded language.[43] Bernal notes many intimate subjects are often deliberately avoided (to avoid disclosure of sexuality, religion and health information) when writing content, this can be determined by communications data analysis.[44] Simply put, your internet activity reveals *everything* you do online (author's emphasis).[45] This also does not even consider factors such as Big Data (where data is *already* aggregated) as Chapter 3 highlighted. In not ruling that communications data adversely affects the essence of the rights, the CJEU automatically reduced the protections available.

d. Effectiveness of data retention

On the appropriateness of data retention, the CJEU noted that data retention was an appropriate means for criminal investigations, and a 'valuable tool.'[46] Marie-Pierre Granger and Kristina Irion pointed out that the CJEU 'tiptoed' around the effectiveness and purposes of the DRD.[47] Orla Lynskey[48] notes that the CJEU does not adequately address whether data retention is a suitable tool to enhance law enforcement.[49] This was the most important omission for Lynskey as there was a lack of detailed 'consideration of whether data retention is in fact appropriate for the purposes of tackling serious crime'[50] in which the CJEU believed that it was. Lynskey, however, questions this belief, referring to the *obiter dictum* from the Czech Constitutional Court (CCC) (which questioned the necessity of data retention),[51] the flawed European

[39] *Tele2 Sverige AB and Watson*, (n3), [99].
[40] ibid, [101].
[41] Matthew White, (n4), 25.
[42] Paul Bernal, 'Data gathering, surveillance and human rights: recasting the debate,' (2016) Journal of Cyber Policy 1:2 243, 248.
[43] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (February 2016), <http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf> accessed 5 April 2017, Paul Bernal, para 3.9, page 132.
[44] ibid, Paul Bernal, para 3.9, page 132.
[45] Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill* (2015-16, HL 93, HC 651) 123.
[46] *Digital Rights Ireland and Seitlinger and Other*s, (n2), [49].
[47] Marie-Pierre Granger and Kristina Irion, (n11), 842.
[48] Orla Lynskey, 'Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Other*: The Good, the Bad and Ugly' (8 April 2014) <http://europeanlawblog.eu/2014/04/08/joined-cases-c-29312-and-59412-digital-rights-ireland-and-seitlinger-and-others-the-good-the-bad-and-the-ugly/> accessed 13 June 2017.
[49] Orla Lynskey, 'The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: *Digital Rights Ireland*' (2014) Common Market Law Review 51: 1789, 1807.
[50] ibid.
[51] The Czech Republic Constitutional Court 2011/03/22 - Pl. ÚS 24/10, [55].

Commission (Commission) statistics,[52] to which the CJEU did not examine.[53] Lynskey continued that given that the CJEU admits the 'particularly serious' interference posed by data retention, 'empirical evidence is needed to sustain the claim that data retention is an appropriate instrument to combat serious crime.'[54] Lynskey's position is supported by the European Data Protection Supervisor (EDPS)[55] who criticised the Commission's statistics as the DRD was based on the *assumption* of necessity.[56] The EDPS also criticised the Commission's assertion that most Member States considered data retention a necessary tool when conclusions were based on just over a third of them,[57] which in fact, were only *statements*.[58] The EDPS further noted that since the DRD was already in place:

> [T]here should be *sufficient qualitative and quantitative information* available which *allows an assessment of whether the measure is actually working and whether comparable results could have been achieved without the instrument or with alternative, less-privacy intrusive means*. Such information should constitute genuine proof and show the relationship between *use* and *result* (author's emphasis).[59]

To which the EDPS concluded that there was not sufficient evidence to demonstrate the necessity, and that further investigations into alternatives should commence.[60]

The EDPS laid further criticism, on the quantitative data, noting crucial information was missing, such as under what circumstances the data was sought, whether all the data accessed was a 'consequence of the legal obligation to retain data or for business purposes'[61] nor were results provided on the *use* of data.[62] Moreover, it was noted it was difficult to draw conclusions as data was only based on information from nine Member States, which are not always fully comparable.[63]

On the qualitative, the EDPS noted that a problem was that not all cases were clear that 'whether use of the retained data was the only means to solve the crime involved.'[64] Further, the EDPS pointed out that while interesting, the use of communications data to exclude suspects and verify alibis, such an argument should be treated with caution as such a position might be misunderstood as implying data retention is 'necessary for proving the innocence of citizens, which would be difficult to reconcile with the presumption of innocence.'[65] In addition to this, the EDPS highlighted that the report does not make comparisons with Member States that did not implement the DRD, or where it was annulled.[66] The EDPS also noted the

---

[52] Commission, 'Report from the Commission to the Council and the European Parliament Evaluation report on the Data Retention Directive (Directive 2006/24/EC)' (18 April 2011) COM(2011) 225 final.
[53] Orla Lynskey, (n49), 1810.
[54] ibid.
[55] Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC) (2011) <http://www.statewatch.org/news/2011/may/edps-opinion-eu-mand-ret-opinion.pdf> accessed 5 June 2017.
[56] ibid, para 38.
[57] ibid, para 40.
[58] ibid, para 41.
[59] ibid, para 43.
[60] ibid, para 44.
[61] ibid, para 45.
[62] ibid.
[63] ibid.
[64] ibid, para 46.
[65] ibid, para 48.
[66] ibid, para 50.

Commission's own admission of the limits of their report and criticised them for not being critical enough of Member States' and relying on statements and not evidence of the necessity of data retention.[67] The UK representatives even admitted to the CJEU that there was no 'scientific data' to underpin the need of data retention which raised the question of what data the DRD had been therefore based upon.[68] This highlights the regrettable acceptance of the appropriateness of data retention by the CJEU.

Another justification made by the CJEU in justifying the appropriateness of retention is regards to Article 6 CFR which guarantees the right of liberty and security.[69] However, the dichotomy between privacy and security has been described as 'miscast,'[70] 'misleading'[71] and 'false,'[72] even if well intentioned[73] because 'measures to protect privacy may improve security'[74] (such as preventing data phishing and identity theft)[75] 'and measures that purport to improve security may in other ways actually reduce that security'[76] (such as exceptional access which would put the security of Internet infrastructure at risk),[77] or even be ineffectual.[78]

e. Did not rule out mass suspicionless surveillance

The CJEU, did not *per se* hold mass surveillance as unlawful, but Lorna Woods argues, it supports the retention of data following justified suspicion, *even perhaps generalised suspicion*, rather than using the analysis of retained data to justify suspicion (author's emphasis). [79] This point is elaborated upon further by Matthew White, who argues that:

---

[67] ibid, para 52.
[68] Monika Ermert, 'EU Data retention might not be proportional to risks' (9 July 2013) <https://policyreview.info/articles/news/eu-data-retention-might-not-be-proportional-risks/170> accessed 4 June 2017.
[69] *Digital Rights Ireland and Seitlinger and Others*, (n2), [42].
[70] Paul Bernal, (n42), 244.
[71] ibid, 245.
[72] Bruce Schneier, 'Security vs. Privacy' (29 January 2008), <https://www.schneier.com/blog/archives/2008/01/security_vs_pri.html> accessed 7 March 2017; Norman Ball, 'Security versus Privacy: A De-Actualizing Formulation' (28 January 2015), <http://www.globalresearch.ca/security-versus-privacy-a-de-actualizing-formulation/5427499> accessed 7 March 2017; Robin Koerner, 'Privacy vs. Security: A False Dichotomy' *HuffPost* (5 April 2014), <http://www.huffingtonpost.com/robin-koerner/privacy-vs-security-a-fal_b_4698157.html> accessed 7 March 2017.
[73] Monica Vilasau, 'Directive 2006/24 / EC on data retention of electronic communications traffic: safety vs. privacy' (2006) IDP. Journal of Internet Law and Policy 0:3.
[74] Paul Bernal, (n42), 244.
[75] Aernout Nieuwenhuis, 'Review of Privacy vs Security' (2015) Utrecht Journal of International and European Law 31:80 137, 138.
[76] Paul Bernal, (n42), 224.
[77] Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter and Daniel J Weitzner, 'Keys under doormats: mandating insecurity by requiring government access to all data and communications' (2015) Journal of Cybersecurity 1, 5.
[78] Fiona O'Cleirigh, 'Bill Binney, the 'original' NSA whistleblower, on Snowden, 9/11 and illegal surveillance' *Computers Weekly* (April 2015) <http://www.computerweekly.com/feature/Interview-the-original-NSA-whistleblower> accessed 7 March 2017; David Bisson, Mass-surveillance 'undermines security' and failed to stop 9/11 attacks, says ex-NSA officer, (6 January 2016), <https://www.grahamcluley.com/mass-spying-undermines-security-failed-stop-911-attacks-says-nsa-officer/> accessed 8 March 2017.
[79] Lorna Woods, (n23).

> Even taking into account the CJEU's ban of general and indiscriminate catch all data retention, this is still profound because suspicion would not be a necessary component for the justification of retention.[80]

This is due to the 'identifiable public' with a direct or indirect relationship with serious crime, and even the data and communication type, persons liable is a much lower threshold than what is required by the ECHR.[81] Moreover, this 'public' was not elaborated upon, nor was the geographical requirement, giving Member States considerable discretion[82] but also raising problems with residence and discrimination.[83]

f. Retention period

The CJEU was silent on the retention period,[84] but AG Saugmandsgaard Øe mistakenly ascribed a six-month period as acceptable[85] based on the GC's judgment in *Roman Zakharov v Russia*, when in fact, the GC referred to a six-month period (of intercept data) as being acceptable in the *individual context* (author's emphasis).[86] The problem of the CJEU's silence is that it creates too much discretion for Member States.

g. The scope of EU law in relation to data retention is limited to the e-Privacy Directive

The application of *Digital Rights Ireland*/*Tele2 and Watson* is limited to the scope of the e-Privacy Directive in that it only concerns publicly available electronic communications services and is limited to traffic and location data.[87] Chapter 3 and 6 demonstrated that data retention in the IPA 2016 includes services and communications data which extend beyond the e-Privacy Directive and therefore, the CJEU's judgments may not strictly be applicable to much of Part 4 of the IPA 2016. Although, there is a contrary view that the CJEU's judgments will have an impact[88] because the CJEU refers to electronic communications and electronic communications services. However, there is no guarantee of this without clarification by the CJEU.

h. UK law not even compatible with EU law

Despite the critique of the CJEU's approach above, questions still remain regarding the UK's implementation of national data retention laws. Niklas Vainio and Samuli Miettinen were unconvinced of the then UK Government's position that the Data Retention and Investigatory Powers Act 2014 (DRIPA 2014) satisfied many of the requirements of *Digital Rights Ireland* as the differences between DRIPA 2014 and the Data Retention (EC Directive) Regulations

[80] Matthew White, (n4), 35.
[81] ibid.
[82] ibid, 26.
[83] ibid, 36.
[84] Matthew White, (n4), 36; Lorna Woods, (n23).
[85] Opinion of Saugmandsgaard Øe, (n1), [243].
[86] *Roman Zakharov*, (n6), [44-48], [260]; Matthew White, 'The new Opinion on Data Retention: Does it protect the right to privacy?' (27 July 2016) <https://eulawanalysis.blogspot.co.uk/2016/07/the-new-opinion-on-data-retention-does.html> accessed 18 June 2017.; Matthew White, (n4), 36.
[87] Anja Møller Pedersen, Henrik Udsen, and Søren Sandfeld Jakobsen, 'Data retention in Europe—the *Tele 2* case and beyond' (2018) International Data Privacy Law 0:0, 3.
[88] ibid, 12, 14.

2009 (DRR) were 'minimal.'[89] The CoA in *Tom Watson and Others*[90] partially[91] ruled that DRIPA 2014 was incompatible with EU whilst avoiding the question of whether DRIPA 2014 permitted blanket indiscriminate data retention.

The powers to require data retention in the IPA 2016 'are broader in every respect than those in'[92] DRIPA 2014. Cobbe argues that the types of communications data retained in IPA 2016 is compatible with EU law because it does not allow the acquisition of knowledge and therefore respects the essence of Article 7 CFR (respect for private and family life, home and communications).[93] However, Cobbe maintained that because EU law now requires a higher standard of security, and for communications data to be retained within the EU, the IPA 2016 falls short on both counts and therefore unjustly interferes with Article 8 CFR (data protection).[94] Moreover, as Cobbe points out, the purposes for which data is to be retained in the IPA 2016, extends beyond serious crime and would thus go beyond what is permitted by *Tele2 and Watson*.[95] Cobbe notes that data retention in the IPA 2016 fails to meet the proportionality requirements of *Digital Rights Ireland* or *Tele2 and Watson* because it can allow telecommunications operators to retain all data indiscriminately, without differentiation, limitation or exception and without safeguards for data subject to professional confidentiality.[96] Additionally, Cobbe notes the IPA 2016 fails to establish a relationship between the data to be retained, the purposes being pursued or any link between that data and public security, nor is the 12 month retention period based on objective criterion and limited to what is strictly necessary.[97] Finally, Cobbe notes that the IPA 2016 does not set out clear and precise rules on the scope and application of data retention, and it does not provide only for retention that is justified as strictly necessary, and therefore disproportionate to Articles 7 and 8 CFR, as it makes data retention the rule and not the exception.[98]

i. UK law incompatible with EU law, but does not permit general and indiscriminate data retention

Both the HC and CoA have ruled that the IPA 2016 and DRIPA 2014 respectively do not permit general and indiscriminate data retention.[99] Both ruled that the CJEU in *Tele2* were referring specifically to Swedish law.[100] However, this has been argued to be a semantic argument[101] 'of distinguishing a catch all power, and a power that can catch all, which of

[89] Niklas Vainio and Samuli Miettinen, 'Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States' (2015) International Journal of Law and Information Technology 23 290, 305.
[90] *Tom Watson and Others*, (n26).
[91] Matthew White, (n27).
[92] Graham Smith, 'Illuminating the Investigatory Powers Act' (22 February 2018) <http://www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html> accessed 22 February 2018. See also Chapters 3 and 6.
[93] Jennifer Cobbe, 'Casting the dragnet- communications data retention under the Investigatory Powers Act' (2018) Public Law 10, 15.
[94] ibid, 15-16.
[95] ibid, 16.
[96] ibid, 19.
[97] ibid.
[98] ibid.
[99] *Liberty v Secretary of State for the Home Department and Others* [2018] EWHC 975, [120-136]; T*om Watson and Others*, (n26), [22-26].
[100] *Liberty*, (n99), [119], [121], [126] and [127]; *Tom Watson*, (n26), [22-3] and [26(2)].
[101] Matthew White, (n27).

course, in any event, amount to the same thing.'[102] The HC felt it impracticable and unnecessary to set out detailed factors to be applied to matters such as national security,[103] despite both the CJEU and ECtHR requiring this.[104] The HC proceeded to consider data retention without due consideration to the ECHR,[105] the next section will demonstrate the problems data retention raises under the ECHR.

7.3 Data Retention under the European Convention on Human Rights

Anthony Speaight QC has twice argued that the ECtHR has never held to preclude general retention for a period.[106] However, the GC of the ECtHR have held that that indiscriminate data retention,[107] indiscriminate capturing of communications[108] and the '[t]he automatic storage for six months of clearly irrelevant data cannot be considered justified under Article 8.'[109]

This Chapter will demonstrate in a comprehensive manner, how data retention under the IPA 2016 violates not only Article 8, but Articles 9-11 and Article 2 Protocol 4. It will further demonstrate how data retention under the IPA 2016 potentially violates Article 6(2)/(3)(c) and all of the mentioned Convention Rights in conjunction with Article 14.

a. Relevant Law

In order to test the compatibility of the UK's data retention regime with the ECHR, it is first necessary to lay out the relevant law from the IPA 2016. Section 87(1) (or Part 4) of the IPA 2016 states that the Secretary of State may issue a retention notice on a telecommunications operator to retain relevant communications data if it is considered necessary and proportionate on approval by a Judicial Commissioner (JC).

The purposes for retention notices in s.61(7) are set out as follows:

> (a) in the interests of national security,
> (b) for the purpose of preventing or detecting crime or of preventing disorder,
> (c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,
> (d) in the interests of public safety,
> (e) for the purpose of protecting public health,
> (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department,

---

[102] Matthew White, 'Data Retention incompatible with EU law: Victory? Victory you say?' (24 May 2018) <https://eulawanalysis.blogspot.com/2018/05/data-retention-incompatible-with-eu-law.html> accessed 21 June 2018.
[103] *Liberty*, (n99), [124].
[104] Matthew White, (n102).
[105] *Liberty*, (n99), [2].
[106] Anthony Speaight, 'Anthony Speaight QC: Charter reach extended, national security hampered, EU competence exceeded' (11 January 2017) <https://judicialpowerproject.org.uk/anthony-speaight-qc-tele2-sverige-charter-reach-extended-national-security-hampered-eu-competence-exceeded/> accessed 22 June 2017; Anthony Speaight, 'Data Retention, National Security and the ECJ: The Continuing Saga' (6 February 2018) <https://judicialpowerproject.org.uk/anthony-speaight-data-retention-national-security-and-the-ecj-the-continuing-saga/> accessed 19 February 2018.
[107] *S and Marper v UK* App nos. 30562/04 and 30566/04 (ECHR, 4 December 2008), [125].
[108] *Kennedy v UK* App no. 26839/05 (ECHR, 18 May 2010), [162].
[109] *Roman Zakharov*, (n6), [255].

(g) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health,
(h) to assist investigations into alleged miscarriages of justice,
(i) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition—
(i) to assist in identifying P, or
(ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition, or
(j) for the purpose of exercising functions relating to—
(i) the regulation of financial services and markets, or
(ii) financial stability.

It must be noted that at the time of writing this Chapter, the UK Government are proposing to amend the purposes for which data communications data can be retained.[110] Section 87(2) stipulates that a retention notice may:

(a) relate to a particular operator or any description of operators,
(b) require the retention of all data or any description of data,
(c) identify the period or periods for which data is to be retained,
(d) contain other requirements, or restrictions, in relation to the retention of data,
(e) make different provision for different purposes,
(f) relate to data whether or not in existence at the time of the giving, or coming into force, of the notice.

Section 87(3) continues that can only be retained for a maximum of 12 months. Section 87(4)(d) notes that:

A retention notice must not require an operator who controls or provides a telecommunication system ("the system operator") to retain data which—
(d) is not retained or used by the system operator for any other lawful purpose.

Section 87(8) notes that a retention notice must specify:

(a) the operator (or description of operators) to whom it relates,
(b) the data which is to be retained,
(c) the period or periods for which the data is to be retained,
(d) any other requirements, or any restrictions, in relation to the retention of the data.

Section 87(9) notes that the requirements or restrictions mentioned in subsection (8)(d) may, in particular, include:

(b) requirements or restrictions in relation to the obtaining (whether by collection, generation or otherwise), generation or processing of—
(i)data for retention, or
(ii)retained data.

[110] The Draft Data Retention and Acquisition Regulations 2018 SI 2018.

Section 89(1) and (2) notes that when a JC approves a decision of the Secretary of State, they must review the necessity and proportionality of their *conclusions* on principles of judicial review. Section 97(1) stipulates that retention notices have extra-territorial application.

Section 61(1)(a), (b) and (c) note that a designated senior office (DSO) of a relevant public authority may obtained communications data for the purposes mentioned in s.61(7) for the purposes of a specific investigation/operation or testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data. Provided that this is necessary and proportionate. Section 62(2)(a) and (b) allows the DSO to authorise any officer of the authority to engage in conduct for the purposes of obtaining data from any person which relates to a telecommunication system or data derived thereof. Section 62(4)(a), (b) and (c) stipulate that this can be done by either obtaining it themselves or asking any person or telecommunications operator the authorised officer believes may be in possession of or is capable of obtaining/disclosing (if not already in possession of it) data. Section 62(5) note that authorisations may relate to data which may or may not already exist at the time of the authorisation, may authorise the obtaining/disclosure of data by persons who are not authorised officers or any conduct which facilitates/enables the obtaining of communications data and may require a telecommunications operator who controls or provides a telecommunication system to obtain/disclose data relating to the use of a telecommunications service provided by another telecommunications operator in relation to that system. Such authorisations are also subject to amendments.[111] Section 263(1) notes that 'data' includes electronic and non-electronic data/information.

b. The Margin of Appreciation and Qualified Rights

The margin of appreciation is described as 'the measure of discretion allowed the Member States in the manner in which they implement the Convention's standards, taking into account their own particular national circumstances and conditions.'[112] The margin of appreciation is most relevant 'for articles containing express limitation clauses.'[113] Chapter 4 already detailed how data retention interfered with Articles 8-11 and Article 2 Protocol 4. The ECtHR has acknowledged that 'interference' with qualified rights must correspond to 'pressing social need,' whether it was 'proportionate to the legitimate aim pursued,' whether the reasons given by the national authorities to justify it are relevant and sufficient...'[114] This was reaffirmed in the later judgment of *Silver and Others v United Kingdom* where the ECtHR expressed that 'those paragraphs of Articles of the Convention which provide for an *exception to a right guaranteed are to be narrowly interpreted* (author's emphasis).'[115]

[111] The Draft Data Retention and Acquisition Regulations 2018 SI 2018.
[112] Arai-Takahashi, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR* (1st edn, Intersentia, Antwerp 2002), 1; Howard C. Yourow, *The Margin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence* (1st edn, Martinus Nijhoff Publishers, 1996), 15; Matthew Saul, 'The European Court of Human Rights' Margin of Appreciation and the Processes of National Parliaments' (2015) Human Rights Law Review 15 745, 746.
[113] Matthew Saul, (n112), 746; Howard C. Yourow, (n112), 15.
[114] For Article 10 see *Sunday Times v United Kingdom* App no. 6538/74 (ECHR, 26 April 1979), [62]; For Article 8 see *S and Marper*, (n107), [101]; For Article 9 see *Fernández Martínez v Spain* App no. 56030/07 (ECHR, 12 June 2014), [124]; For Article 11 see *Kudrevičius and Others v Lithuania* App no. 37553/05 (ECHR, 15 October 2015), [143]; For Article 2 Protocol 4 see *Khlyustov v Russia* App no. 28975/05 (ECHR, 11 July 2013), [84].
[115] *Silver and Others v UK* App nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 and 7136/75 (ECHR, 25 March 1983), [97(d)].

The ECtHR has noted that while it is for the national authorities to make the initial assessment in all these respects, the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention.[116] Nevertheless, a margin of appreciation must be left to the competent national authorities in this assessment. The breadth of this margin varies and depends on a number of factors including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference and the proportionality and pressing social need of the issue. The margin will tend to be *narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights* (author's emphasis). Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted.[117] Given that Chapter 3 highlighted the seriousness of interference with a *collection* of Convention Rights, which are crucial to effective enjoyment of online/offline freedom, and in some cases very important for an individual's identity the margin should be particularly narrow. The ECtHR has stressed on more than one occasion that the 'protection of personal data is of *fundamental importance* to a person's enjoyment of his or her right to respect for private and family life' and 'that the *need for such safeguards is all the greater when it comes to protecting personal data subject to automatic processing, especially when these data are used for police purposes* (author's emphasis).'[118]

7.4 Is Data Retention in accordance with the/prescribed by law?

Articles 8-11 and Article 2 Protocol 4 are known as qualified rights due to the fact that the state can set limitations upon them in certain circumstances (margin of appreciation). Interferences with Article 8 and Article 2 Protocol 4 have to be 'in accordance with the law' whereas with Articles 9-11, interferences have to be 'prescribed by law.' In the partly dissenting opinions of Loucaides and Judge Jočienė, they noted the link between the two terms.[119] It has also been noted that the expressions are recognised as being similar, the same,[120] and identical.[121] Therefore, when considering the 'quality of the law'[122] this will apply uniformly amongst the qualified rights in question. From here on in, 'in accordance with the law' will also mean 'prescribed by law.'[123]

The ECtHR have noted that the wording 'in accordance with the law' requires the impugned measure to have some basis in domestic law.[124] This also relates to the 'quality of the law' requiring it 'to be compatible with the rule of law, a concept inherent in *all the Articles of the Convention* (author's emphasis).'[125] It also should be accessible to the person concerned and foreseeable as to its effects.[126]

---

[116] *S and Marper*, (n107), [101].
[117] ibid, [102].
[118] *S and Marper*, (n107), [103]; *B.B. v France* App no. 5335/06 (ECHR, 17 December 2009), [61]; *M.K. v France* App no. 19522/09 (ECHR, 18 April 2013), [35].
[119] *Kafkaris v Cyrprus* App no. 21906/04 (ECHR, 12 February 2008).
[120] *Rekvényi v Hungary* App no. 25390/94 (ECHR, 20 May 1999), [59]; See also *Niyazov v Russia* App no. 27843/11 (ECHR, 16 October 2012), [116].
[121] *Telegraaf and Others v the Netherlands* App no. 39315/06 (ECHR, 22 November 2012), [89].
[122] *Rekvényi*, (n120), [59].
[123] Joint Committee on Human Rights, *First Report* (2000-01), HL 42/HC 296), Annex 2.
[124] *M.M. v UK* App no. 24029/07 (ECHR, 24029/07), [193]; *S and Marper*, (n107), [95].
[125] *Stafford v United Kingdom* App no. 46295/99 (ECHR, 28 May 2002), [63].
[126] *Amann v. Switzerland* App no. 27798/95 (ECHR, 16 February 2000), [50]; *S and Marper*, (n107), [95]; *Malone v UK* App no. 8691/79 (ECHR, 2 August 1984), [67].

A. Accessibility

The ECtHR has noted, that publication of the law is likely to meet accessibility.[127] Paragraph 4, Schedule 9 of the IPA 2016 allows retention notices to be made for up to three months after JCs are appointed. The most problematic provision on retention notices in this regard is s.87(2)(e) which allows the Secretary of State to make different provision for different purposes. Provisions, and purposes are nowhere defined within Part 4, thus making this particular aspect unclear and problematic. Moreover, (as of writing this thesis), there is no Code of Practice to further clarify the matter, which the ECtHR regards as very important.[128]

In *Liberty v UK* regarding the issue of arrangements to be made by the Secretary of State in relation to external communications under the old Interception of Communications Act 1985 (ICA 1985), the ECtHR noted that 'that *details of* these *"arrangements"* made under section 6 were *not contained in legislation* or *otherwise made available to the public* (author's emphasis).'[129] This would mean that *at the relevant time* the IPA 2016 did not 'set out in a form accessible to the public any indication'[130] as to what provisions the Secretary of State could make, and the purposes for them, therefore, not open to public knowledge or scrutiny.[131] Whilst finding a violation in *Liberty* for UK law not being 'in accordance with the law'[132] the ECtHR noted that despite the then Commissioner in annual reports concluding that arrangements had been complied with, this did 'not contribute towards the accessibility and clarity of the scheme, since he was not able to reveal what the "arrangements" were.'[133] This would be no different under the new Investigatory Powers Commissioner (IPC) who is not required[134] to publish reports on retention notices,[135] and in any event only produces annual reports on JCs.[136]

Therefore, even with a Code of Practice in place and a clarification on s.87(2)(e), *up until that point*, s.87(2)(e) of the IPA 2016 does not satisfy accessibility. A finding of a law failing to satisfy the 'in accordance with the law' criteria 'obviates the need for the Court to determine whether the interference was "necessary in a democratic society" for one of the aims enumerated therein.'[137] However, it is contented that it is necessary and possible[138] to progress through to the requirement of foreseeability in order to demonstrate how deeply flawed much of s.87 becomes under deeper scrutiny.

B. Foreseeability

A rule is 'foreseeable' if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct.[139] This is to ensure that there is

[127] *Leander v Sweden* App no. 9248/81 (ECHR, 26 March 1987), [52-3].
[128] *Kennedy*, (n108), [169].
[129] *Liberty v UK* App no. 58243/00 (ECHR, 1 July 2008), [66].
[130] ibid, [69].
[131] *Shimovolos v Russia* App no. 30194/09 (ECHR, 21 June 2011), [69].
[132] *Liberty*, (n129), [69-70].
[133] ibid, [67].
[134] See s.234(2)(d) of the IPA 2016.
[135] Though it is possible if the Prime Minster requests this, or the IPC decides to do so, see s.234(3) and (4) respectively.
[136] See s.234(1) of the IPA 2016.
[137] *M.M.*, (n124), [207]; *Amann*, (n126), [63].
[138] *Kurić and others v Slovenia* App no. 26828/06 (ECHR, 12 March 2013), [350].
[139] *Amann*, (n126), [56].

adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any such measures,[140] thus, allowing individuals to avoid exposure to unwelcome intrusions by the State.[141]

In *Zakharov*, the GC reiterated that foreseeability in the context of interception cannot be the same as other fields.[142] For the GC, foreseeability in the special context of secret surveillance, which extends to measures *such as* (including data retention)[143] the interception of communications.[144] The GC did note that, foreseeability 'cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly.'[145] The GC noted that where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident.[146] Therefore, the law needs to be particularly precise,[147] a position agreed upon by the Constitutional Courts of Romania[148] and the Czech Republic.[149] It is also *essential* to have clear, binding[150] detailed rules, especially as the technology available for use is continually becoming more sophisticated (author's emphasis).[151] This sentiment was echoed by the ECtHR in *Szabo* where it was noted that:

> Given 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 protection of private life even more acutely* (author's emphasis).[152]

Furthermore, the ECtHR in *Szabo* noted that the guarantees required by the extant Convention case-law on interceptions *need to be enhanced* so as to address the issue of such surveillance practices (author's emphasis).[153] Moreover, regarding foreseeability:

> In its case-law on secret measures of surveillance, the Court has developed the following *minimum safeguards* that should be set out *in **statute** law in order to avoid abuses of power*: the *nature of offences* which may give rise to an interception order; *a definition of the categories of people liable* to have their telephones tapped; *a limit on the duration* of telephone tapping; the *procedure to be followed for examining, using and storing the data obtained*; the *precautions* to be taken *when communicating the*

[140] *Uzun v Germany* App no. 35623/05 (ECHR, 2 September 2010), [61].
[141] Privacy International, 'Memorandum of Laws Concerning the Legality of Data Retention with regard to the Rights Guaranteed by the European Convention on Human Rights' (10 October 2003) <http://www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf> accessed 25 June 2017, p3.
[142] *Roman Zakharov*, (n6), [229].
[143] *S and Marper*, (n107), [99].
[144] *Roman Zakharov*, (n6), [229].
[145] ibid.
[146] ibid.
[147] *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* App no. 62540/00 (ECHR, 28 June 2007), [75].
[148] Romania Constitutional Court DECISION no.12581 from 8 October 2009.
[149] The Czech Republic Constitutional Court, (n51), [37].
[150] *Valenzuela Contreras v Spain* App no. 27671/95 (ECHR, 30 July 1998), [60]; 'For this purpose, the rules need not be statutory, provided that they operate within a framework of law and that there are effective means of enforcing them.' *Catt and T, R (on the applications of) v Commissioner of Police of the Metropolis* [2015] UKSC 9, [11].
[151] *Roman Zakharov*, (n6), [229].
[152] *Szabo and Vissy v Hungary* App no. 37138/14 (ECHR, 12 January 2016), [53].
[153] ibid, [68-70].

> *data to other parties*; and the *circumstances in which recordings may or must be erased or destroyed* (author's emphasis)…
>
> Furthermore, there must be a measure of *legal protection* in domestic law *against arbitrary interference* by public authorities with the rights safeguarded by Article 8 § 1. Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident. Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, *it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power*. Consequently, *the law must indicate the scope of any such discretion conferred on the competent authorities* and *the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference*…[154]

It is important to note that although the ECtHR has held that Code of Practices are very important with regards to legality, they are not binding, nor are they set out in statute as the ECtHR regards as a minimum. Therefore, even *if* as mentioned in section 7.4(A) the Codes of Practice are now in force, this cannot be said to prevent abuses of power or arbitrary interferences with Article 8 because they are not set out in statute nor are they legally binding. Therefore, it cannot be said that combining Codes of Practices with Part 4 sufficiently ensures foreseeability.

Continuing with foresseability, Judge Pinto de Albuquerque, in his partly concurring/dissenting opinion, argued further in *Draksas* adding the degree of reasonable suspicion required for a surveillance measure, notification and special guarantees with regards to special communications i.e. lawyer-client etc are all necessary in determining whether a measure sufficiently clear.[155] Reasonable suspicion,[156] notification,[157] and special guarantees regarding special communications[158] are guarantees that has been endorsed (as will be discussed below) by the ECtHR in judgments.

AG Saugmandsgaard Øe and the CJEU agreed that general data retention obligations poses just as serious of an interference (in the individual context) as interception and greater risks with access (see above).[159] Given that Chapter 3 thoroughly illustrates that communications data is *at least* just as serious of an interference as interception (with some communications data *requiring* interception), the ECtHR accepting this position and given that Chapter 5 demonstrates how and why data retention is a measure of (mass) secret surveillance, the same safeguards regarding secret surveillance *must* apply.[160] Moreover, given the gravity of interference, not just with Article 8, but Articles 9-11 and Article 2 Protocol 4, these strict standards must be maintained,[161] irrespective of the fact that data retention is generalised surveillance.[162]

---

[154] *Sefilyan v Armenia* App no. 22491/08 (ECHR, 2 October 2012), [125-6].
[155] *Draksas v Lithuania* App no. 36662/04 (ECHR, 31 July 2002).
[156] *Roman Zakharov*, (n6), [260].
[157] ibid, [286-302].
[158] *Kopp v Switzerland* App no. 23224/94 (ECHR, 25 March 1998), [73-5].
[159] Matthew White, (n4), 25.
[160] ibid, 33-4.
[161] *Uzun*, (n140), [66].
[162] *Liberty*, (n129), [63].

1. Unfettered and Arbitrary Interferences

The HC in *Davis* with regards to retention notices under DRIPA 2014, acted on the assumption that a telecommunications operator would be required to retain *all communications data for a period of 12 months*, a general retention regime (author's emphasis).[163] Moreover, s.87(2)(a) and (b) theoretically allows for the possibility 'all operators in the UK to be required to retain all data of users and subscribers'[164] and thus should be treated as a blanket and indiscriminate power.[165] Although the Home Office assured that they 'certainly [would] not place obligations on every one of [the "200 or 300" communications service providers]'[166] and the HC (in a later judgment) not conceiving how the tests of necessity and proportionality would permit general indiscriminate data retention,[167] '[i]t is the *potential reach of the power* rather than its actual use *by which its legality must be judged* (author's emphasis).'[168] All are potentially subject to this power and insufficient legal restraints does not become legal simply because self-restrain may be exercised.[169] Simply put, it is not the application of the power that should be questioned, but the power itself. When it cannot be ruled out that national legislation can be taken to enable so-called strategic, large-scale interception/surveillance, it becomes a matter of concern.[170] Given that Chapter 6 highlighted that retention obligations can be imposed upon essentially anything that can communicate, whether it be an Internet Service Provider (ISP), webmail provider, software vendor or anything under the umbrella of the Internet of Things (IoT), it must be concluded that 'that the legislation *directly affects all users of communication systems and all homes* (author's emphasis).'[171]

When the UK Government in *Liberty* admitted that it was possible for any person who sent/received *any form* of telecommunication *outside* the British Islands to have their communications intercepted, the ECtHR noted that the capture of external communications was *virtually unfettered* (author's emphasis).[172] Just as s.97(1) noted, retention notices have extra-territorial application, and thus not only has the potential to capture communications data of everyone within the UK, but is also possible to capture communications data of everyone *outside* the UK. Whether it is the UK or abroad, s.87(2)(a) and (b) in combination with s.97(1) is nothing short of a *virtually unfettered* blanket indiscriminate power.

Abu Bakar Munir and Siti Hajar Mohd Yasin noted '[t]he requirement of foreseeability is not satisfied by blanket regulations…that allow everyone to foresee that the State will interfere with their right to a private life.'[173] Therefore, in other words, data retention occurs, and affects the fundamental rights of individuals *irrespective* of conduct.[174] This position has been echoed

[163] *Davis & Ors, R (on the application of) v Secretary of State for the Home Department & Ors* [2015] EWHC 2092, [65].
[164] Matthew White, (n4), 26.
[165] Matthew White, (n27); Jennifer Cobbe, (n93), 18; Andrew D. Murray, 'Data transfers between the EU and UK post Brexit?' (2017) International Data Privacy Law 7:3 149, 161.
[166] Science and Technology Committee, *Investigatory Powers Bill: technology issues* (2015-16 HC 573), para 15.
[167] *Liberty*, (n99), [129].
[168] *Beghal v DPP* [2015] UKSC 49, [102].
[169] ibid.
[170] *Szabo*, (n152), [69].
[171] ibid, [38].
[172] *Liberty*, (n129), [64].
[173] Abu Bakar Munir and Siti Hajar Mohd Yasin, 'Retention of Communications Data: A Bumpy Road Ahead' (2004) J. Marshall J. Computer & Info. L. 22:4 731, 755; Privacy International, (n141), p8.
[174] Matthew White, 'The new Opinion on Data Retention: Does it protect the right to privacy?,' (n86); *Nada v Switzerland* App no. 10593/08 (ECHR, 12 September 2012), [182] 'Thus, in order to ensure "respect" for

by the Austrian Constitutional Court (ACC) where it noted that data retention '*affects almost exclusively persons who do not give rise to a cause for data retention*' meaning *nothing in their conduct would require state intervention* as the overwhelming majority use services to *exercise* their fundamental rights i.e. freedom of expression, information and communication (author's emphasis).[175] The German Federal Constitutional Court (GFCC) noted that data retention laws 'does not give the citizen a regular possibility of avoiding storage.'[176] The Romanian Constitutional Court (RCC) noted that law must be accessible, clear, predictable and unambiguous and there 'must have a clear representation of the applicable legal provisions, in order to adapt their conduct and to foresee the consequences that may occur from their breach.'[177] The CCC noted that legal regulations *must* be precise and unambiguous while also being *sufficiently predictable* so that it can provide the potentially affected individuals *with sufficient information on the circumstances and conditions* under *which the public authority is entitled to interfere with their privacy* and *so that they can act accordingly in order to avoid conflict with the restricting norm* (author's emphasis).[178] The CJEU in *Digital Rights Ireland*[179] and AG Saugmandsgaard Øe acknowledged that 'the vast majority of the data retained will relate to persons who *will never be connected in any way* with serious crime (author's emphasis).'[180]

The GC has previously noted that 'legal provisions which allowed an unfettered discretion…[do]… not meet the required standards of clarity and foreseeability'[181] and thus results in a violation.[182] Indiscriminate data capture is also contrary to Article 8[183] as it subjects 'every citizen to the certainty of ongoing and unremitting interference in his or her private life.'[184] Thus, without even considering other potential limiting aspects of s.87, it becomes clear that data retention envisaged in this section has the potential to be blanket and indiscriminate,[185] (just as DRIPA 2014 was) and therefore incompatible with foreseeability and thus not in accordance with the law.

In *Mustafa Sezgin Tanrikulu v Turkey* the Turkish intelligence agency (MIT) had obtained permission by the Diyarbakır Assize Court:

> [T]o intercept all domestic or international telephone calls and communications… to obtain information contained in SMS, MMS, GPRS and fax communications, as well as caller IDs, correspondents' IP addresses and all other communication-related information.[186]

---

private and family life within the meaning of Article 8, the realities of each case must be taken into account *in order to avoid the mechanical application of domestic law to a particular situation*.' A mechanical application of law occurs *regardless* of the situation.

[175] Austrian Constitutional Court, Decision G 47/2012-49, G 59/2012-38, G 62/2012-46, G 70/2012-40, G 71/2012-36 27 June 2014, [2.3.14.4].

[176] BVerfG, judgment of the First Senate of 02 March 2010 - 1 BvR 256/08 - Rn. (1-345), [210].

[177] Romania Constitutional Court, (n148).

[178] The Czech Republic Constitutional Court, (n51), [37].

[179] *Digital Rights Ireland and Seitlinger and Other*s, (n2), [58].

[180] Opinion Saugmandsgaard Øe, (n1), [252].

[181] *Hasan and Chaush v Bulgaria* App no. 30985/96 (ECHR, 26 October 2000), [86].

[182] ibid, [89].

[183] *Kennedy*, (n108), [160] and [162]; *Szabo*, (n152), [69].

[184] Privacy International, (n141), p9.

[185] Matthew White, (n27); Matthew White, (n4), 26; Jennifer Cobbe, (n93), 18.

[186] *Mustafa Sezgin Tanrikulu v Turkey* App no. 27473/06 (ECHR, 18 July 2017), [7].

This permission lasted nearly two months.[187] Excluding the actual phone calls, Table A from Chapter 3 highlights that MIT were allowed to obtain all the communications data that the Home Office listed to the Joint Committee on the Draft Investigatory Powers Bill (JCDIBP).[188] Therefore, the findings of the ECtHR become crucial due to the measure being applicable to everyone within a particular jurisdiction.[189] Although the ECtHR ruled in this specific case that Diyarbakır Assize Court's decision did not even satisfy the requirements of Turkish law,[190] and was therefore, not 'in accordance with the law'[191] their reasoning is important. First, the decision 'was not limited to people suspected of the criminal offences'[192] laid down in Turkish law. Secondly, the decision did not contain any findings or strong indicators of crime, only making references to activities covered by Turkish law, nor did it specify which factors had been taken into account for determining that there were strong indications those crimes had been committed.[193] And finally, the decision did not try determine whether the aims in question could not be achieved by other, less intrusive, means.[194] Retention notices suffer the same problems (particularly the first and second), especially with the extra-territorial effect in that 'conduct' and 'persons' outside the UK is not defined, thus highlighting they would not be 'in accordance with the law.'

2. Unfettered powers that are sporadically used

As noted above, when the Home Office gave evidence to the Science and Technology Committee, they noted that that obligations to retain would not be imposed on all telecommunications operators. Such a position could satisfy the requirements of *Tele2 and Watson* because it could be argued not to be a 'catch all' power.[195] However, as Lord Kerr's dissent highlights 'an unfettered power which may be arbitrarily or capriciously used does not become legal just because people generally do not take exception to its use.'[196] It will be highlighted even if a retention notice was issued on just *one* telecommunications operator, the requirement of foreseeability would still not be met. As the Council of Europe's Commissioner for Human Rights (Commissioner HR) noted that 'suspicion less *mass retention* of communications data is fundamentally contrary to the rule of law.'[197] What this demonstrates is that, according to the Commissioner HR, data retention does not have to be blanket, the measure just has to be encompassed on a large scale for it to be unlawful, a discriminatory indiscriminate power.[198] This subsection will attempt to demonstrate why this is the correct view under the ECHR.

i. Nature of the offences

[187] ibid.
[188] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n43), Home Office, pages 515-517.
[189] *Mustafa Sezgin Tanrikulu*, (n186), [57].
[190] ibid, [60].
[191] ibid, [64-65].
[192] ibid, [57].
[193] ibid, [58].
[194] ibid, [59].
[195] Matthew White, (n4), 25-7.
[196] *Beghal*, (n168), [101].
[197] Council of Europe's Commissioner for Human Rights, 'The rule of law on the Internet and in the wider digital world' (2014) <https://rm.coe.int/16806da51c> accessed 14 July 2017, para 6, p22.
[198] Matthew White, (n4), 38.

It still has to be assumed that all data from one telecommunications operator is retained for 12 months, in line with the HC in *Davis*, White, Cobbe and Murray. Given that one of the requirements for foreseeability is for there to be sufficient detail regarding the nature of offences that give rise to a surveillance measure, it is important to consider the purposes for data retention set out in s.61(7).

a. In the interests of national security

Speaight suggests that, national security grounds could be invoked to bypass EU law and implement a 'catch all' blanket indiscriminate data retention.[199] The European Parliament rejects such notion,[200] moreover, as *Schrems* demonstrates, national security cannot be used as a 'trump card' even for 'third-countries.'[201] The Investigatory Powers Tribunal (IPT) has sought clarification by the CJEU of *Tele2 and Watson* in the national security context.[202] That judgment, however, fails to consider the wider context of fundamental human rights protection in the context of mass surveillance.[203] Where the CFR may not apply[204] (for example, national security),[205] due to its application being narrower,[206] the ECHR would,[207] and '[t]he ECtHR could alternatively also solve the issue with the national legislation on data retention' legality under Article 8 ECHR.[208] In any event, national security grounds for data retention would fall foul of Article 8(2) for the reasons mentioned in sections 7.2(A) and (B) due to failures of accessibility and particularly foreseeability.

Therefore, it is important to consider the grounds of national security itself. Lack of clarity on national security for data retention was already highlighted by the RCC.[209] The UN Special Rapporteur on Freedom of Expression, Frank LaRue regards national security as '[v]ague and unspecified' and the use of the amorphous concept to justify invasive limitations on human rights is concerning because it is vulnerable to state manipulation.[210] Nearly two decades prior

[199] Anthony Speaight, 'Anthony Speaight QC: Charter reach extended, national security hampered, EU competence exceeded,' (n106).
[200] European Parliament, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, 21 February 2014 (2013/2188(INI)), para 16.
[201] Case C-362/14 *Schrems* [2015] ECR-I 650.
[202] *Privacy International v the Secretary of State for Foreign and Commonwealth Affairs and Others* [2017] IPT/15/110/CH, [72].
[203] Matthew White, 'The Privacy International case in the IPT: respecting the right to privacy?' (14 September 2017) <https://eulawanalysis.blogspot.co.uk/2017/09/the-privacy-international-case-in-ipt.html> accessed 20 September 2017.
[204] European Commission Legal Services Opinion, 'Committee on Civil Liberties, Justice and Home Affairs Legal Opinion - Question relating to the judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* - Directive 2006/24/EC on data retention - Consequences of the judgment' (2014) <http://www.statewatch.org/news/2015/apr/ep-ls-opinion-digital-rights-judgment.pdf> accessed 13 June 2017, para 104.
[205] Anthony Speaight, 'Anthony Speaight QC: Charter reach extended, national security hampered, EU competence exceeded,' (n106).
[206] House of Lords European Union Committee, *The UK, the EU and a British Bill of Rights; (12th Report)* (2015-16 HL 139), para 71.
[207] European Commission Legal Services Opinion, (n204), para 81; Case C-127/08, *Metock v Minister of Justice, Equality and Law Reform* [2008] ECR I-06241, [74-9].
[208] Elitsa Stoeva, 'The Data Retention Directive and the right to privacy' (2014) ERA Forum 15:4 575.
[209] Romania Constitutional Court, (n148).
[210] Frank La Rue, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (17 April 2013) <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf> accessed 26 July 2017, paras 58 and 60.

to this, judge Pettiti in *Kopp* uttered that numerous European States have failed to comply with Article 8 abusing concepts such as national security, by distorting the meaning and nature of that term.[211] Pettiti recommended that some clarification was needed in order to refine and improve the system for the prevention of terrorism.[212] In *Roman Zakharov*, the GC acknowledged that foreseeability cannot mean States must enact 'provisions listing in detail all conduct that may prompt a decision to subject an individual to secret surveillance on "national security" grounds.'[213] This is due to national security varying in character or being difficult to define in advance.[214] The GC noted, however, at the same time, reiterated that this does not permit States to have unfettered power. Even in the national security context, the GC noted that Member States only enjoy a certain margin of appreciation and that[215] the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to prevent arbitrary interferences.[216] The GC noted it was 'significant' that Russian law did 'not give any indication of the circumstances under which an individual's communications may be intercepted on account of events or activities endangering Russia's national…security.'[217] This left:

> [A]uthorities an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse.[218]

The failure to define 'national security' was also highlighted by the ECtHR in *Iordachi*.[219] In the UK, although there is no exhaustive definition of national security, the Interception of Communications Commissioner (IoCCO) in his 1986 Report defined it as activities 'which threaten the safety or well-being of the State, and which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means'[220] which the ECtHR accepted.[221] Though, this may be problematic as it is not binding.[222] The UK House of Lords (UKHoL) in *Rehman* highlighted some potential characteristics of national security.[223] The Information Tribunal in *Baker* summarised this as follows:

(i) "national security" means "the security of the United Kingdom and its people.";
(ii) the interests of national security are not limited to action by an individual which can be said to be "targeted at" the UK, its system of government or its people;
(iii) the protection of democracy and the legal and constitutional systems of the state is a part of national security as well as military defence;
(iv) "action against a foreign state may be capable indirectly of affecting the security of the United Kingdom"; and

[211] *Kopp*, (n158).
[212] ibid.
[213] *Roman Zakharov*, (n6), [247].
[214] ibid.
[215] ibid, [232].
[216] Ibid, [247].
[217] ibid, [248].
[218] ibid.
[219] *Iordachi v Moldova* App no. 25198/02 (ECHR, 10 February 2009), [46].
[220] *Kennedy*, (n108), [33].
[221] ibid, [159].
[222] *Valenzuela Contreras*, (n150), [60].
[223] *Secretary of State for the Home Department v Rehman* [2001] UKHL 47, [14-17], [50].

(v) "reciprocal co-operation between the United Kingdom and other states in combating international terrorism is capable of promoting the United Kingdom's national security"[224]

The IPA 2016, however, makes no reference to the IoCCO's Report, *Rehman* or *Baker* regarding national security, despite the Joint Committee on the Draft Investigatory Powers Bill (JCDIPB) recommending that national security should be defined.[225] Baroness Jones of Moulsecoomb attempted[226] to introduce a definition during the IPA 2016's passage, but was rejected and was subsequently withdrawn.[227] Baroness Jones did note 'if you have not described it, how can you be sure that you are doing the right thing?'[228] because '[n]ational security as a legal test is *absolutely meaningless* if left without a statutory definition' (author's emphasis).[229]

Even without a definition of national security the ECtHR still holds that the law in question should specify the circumstances in which an individual may be at risk of surveillance on *those grounds*.[230] In *Zakharov*, the GC acknowledged that prior judicial authorisation, may act as a sufficient safeguard when definitions are lacking detail.[231] For this safeguard to be sufficient, the GC ruled that secret surveillance should not be ordered 'haphazardly, irregularly or without due and proper consideration.'[232] The GC noted, in making this assessment, consideration will be given to the authority authorising surveillance, its scope of review and content of authorisation.[233] When national security is at stake which affects fundamental rights, they must be subject to some form of adversarial proceedings before an independent body able to review reasons for decisions.[234] Further, this independent body must be able to react in cases where invoking that concept has no reasonable basis in the facts or reveals an interpretation of "national security" that is unlawful or contrary to common sense and arbitrary.[235]

The first safeguard the GC referred to in *Zakharov* was the prevention of arbitrary or *indiscriminate* secret surveillance.[236] Reasoned requests with supporting material from the requesting authority, and the fact that a judge must give reasons for authorisations is also an important safeguard.[237] The scope of review, the GC reiterated that it must be capable of verifying the existence of *a reasonable suspicion* against the *person* concerned. This included, in particular, whether there are *factual* indications for suspecting a person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures e.g. which engagers national security.[238] Such requests for surveillance

[224] *Norman Baker v the Information Commissioner and the Cabinet Office* [2006] EA/2006/0045, [26].
[225] Joint Committee on the Draft Investigatory Powers Bill, (n45), para 691.
[226] Investigatory Powers Bill HL Bill (2016-17) 40—VI 56/2, cl 236A.
[227] HL Deb 12 September 2016, vol 774, col 1315-1319.
[228] ibid, col 1319.
[229] ibid, col 1315.
[230] *Iordachi*, (n219), [46].
[231] *Roman Zakharov*, (n6), [249].
[232] ibid, [257].
[233] ibid.
[234] *Al-Nashif v Bulgaria* App no. 50963/99 (ECHR, 20 June 2002), [123]; *Janowiec and Others v Russia* App nos. 55508/07 and 29520/09 (ECHR, 21 October 2013), [213-214].
[235] *Al-Nashif*, (n234), [124]; *C.G. and others v Bulgaria* App no. 1365/07 (ECHR, 24 April 2008), [40];
[236] *Roman Zakharov*, (n6), [259].
[237] ibid.
[238] ibid, [260].

measures must also be necessary in a democratic society, proportionate to the legitimate aim pursued i.e. least restrictive measure.[239]

For the purposes of the IPA 2016, judicial control comes under power of JC's. It must be noted that JC's review of retention notices fail the first requirement that surveillance measures must not be arbitrary or indiscriminate. Whether retention notices are issued on all telecommunications operators, or just one, the potential communications data to be retained is *all* for 12 months in each case. As the GC has noted, it would be contrary to the rule of law if discretion was granted to even judges in terms of an unfettered power.[240] An unfettered power as described in section 7.4(B)(1), would not satisfy the requirements of foreseeability.

As noted above, JC's can only consider retention notices on judicial review principles. There is, however, concerns with the JC's being solely confined to principles of judicial review as it is much less stringent than judicial authorisation[241] and is more restrictive as judges are unlikely to stray beyond conventional *Wednesbury* principles.[242] Judicial review principles are even more constrained in the context of national security pre-Human Rights Act 1998 (HRA 1998), with very little changing post-HRA 1998.[243] The Information Tribunal noted that even in ECHR territory, judges operating judicial review principles are not to act as second-stage administrators,[244] and in the national security context a 'no less, but no more'[245] approach was adopted. This is despite, the adjudicatory role of courts in human rights and judicial review cases being different. With the former, the *merits* are considered,[246] however, the latter, it has been criticised by partly dissenting judges' Walsh and Russo for a *lack of* merits review (author's emphasis).[247] The IPC has offered assurances, but this will be considered in subsection 7.6(C)(c)(f).

Another problem with the JC's review process is that s.89(1) only permits the JC's to review the Secretary of State's *conclusions*. There is no obligation on the Secretary of State to make a full and frank disclosure (like with judicial authorisation) to the JC, and therefore, JC's could be misled, and would in any event be unable to give rigorous and critical analysis.[248] David Anderson noted that he had private assurances that JC's would receive the same evidence as the Secretary of State, but this cannot be guaranteed because it is not present on the face of the

[239] ibid.
[240] ibid, [230]; Matthew White, (n4), 38.
[241] *Mills & Anor, R (on the application of) v Sussex Police & Anor* [2014] EWHC 2523, [26]. The requirements for judicial authorisation are as follows; 1. Granting warrants must only be sought as a last resort and should not be employed where less draconian measures can achieve that objective. 2. *Full and frank disclosure to the judge*, even where it might prove adverse to the application. 3. Duty not to mislead a judge. 4. Granting resides with a judge who must bring a *"rigorous and critical analysis"* to the application and *satisfy himself or herself* that the material provided justifies the grant of the warrant. 5. The judge ought to give *reasons for decisions made*. 6. The application must not be made for an ulterior purpose.
[242] Matthew White, (n4), 29.
[243] Roger Masterman, 'Rebalancing the Unbalanced Constitution: Juridification and National Security in the United Kingdom' in Fergal F. Davis and Fiona de Londras (eds), *Critical debates on counter-terrorist judicial review* (Cambridge University Press 2014).
[244] *Baker v Secretary of State for the Home Department* [2001] UKIT NSA2 [53-56].
[245] ibid, [76].
[246] Matthew White, (n4), 30.
[247] *Vilvarajah and Others v UK* - App nos. 13163/87; 13164/87; 13165/87; 13447/87; 13448/87), 30/10/1991, (ECHR, 30 October 1991) [3].
[248] Matthew White, (n4), 30.

IPA 2016.[249] Even if the JC's received the same evidence as the Secretary of State, this could in effect amount to 'a summary of a summary of a summary of a summary of a summary of the original intelligence case.'[250] The GC in *Zakharov* ruled it *essential* that the supervisory body has 'access to all relevant documents, including closed materials' and 'that all those involved in' surveillance 'activities have a duty to disclose to it any material it required.'[251] There is no requirement of the JC's to give reasons for allowing a retention notice, only their refusal, nor is there any requirement to verify the existence of a reasonable suspicion (discussed below) which is contrary to *Zakharov*.[252]

There is a lack of adversarial process with regards to issuing retention notices, even with judicial authorisations.[253] Lord Pannick,[254] and Byron Karemba[255] both articulate for an adversarial process (e.g. use of special advocates which is already the case for national security in the immigration context) if at least to allow the JC's to hear contrasting views as to intensity of what review applies.[256] Even if this were the case, questions of the JC's independence remain.[257]

Finally, and possibly the greatest threat of arbitrary data retention on grounds of national security comes not from Part 4, but Part 3 of the IPA 2016. Chapter 6 highlighted how s.61(1) and (2) in conjunction with s.61(7)(a) gives designated senior officers (DSO's) of police forces, security services and many others[258] powers to authorise any officer (or who is *not* an authorised officer)[259] to obtain data from *any person* which relates to a telecommunication system, or data derived from a telecommunication system for national security purposes

[249] ibid, 31.
[250] ibid, 30-1.
[251] *Roman Zakharov*, (n6), [281].
[252] ibid, [259-260].
[253] T.J. McIntyre, (n16).
[254] David Pannick, 'David Pannick: Safeguards provide a fair balance on surveillance powers' *The Times* (London, November 12 2015) <http://www.thetimes.co.uk/tto/law/article4611174.ece> accessed 18 July 2017.
[255] Byron Karemba, 'The Investigatory Powers Bill: Putting the Investigatory Powers Commissioner in Focus (Part II)' (15 April 2016) <https://ukconstitutionallaw.org/2016/04/15/byron-karemba-the-investigatory-powers-bill-putting-the- investigatory-powers-commissioner-in-focus-part-ii/> accessed 13 July 2017.
[256] ibid; Joint Committee on the Draft Investigatory Powers Bill, *oral evidence*, 16 December 2015, < https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf> accessed 13 July 2017.
[257] Matthew White, (n4), 32-3.
[258] Schedule 4 details the relevant public authorities capable of using this power. This includes Police force maintained under section 2 of the Police Act 1996, Metropolitan police force, City of London police force, Police Service of Scotland, Police Service of Northern Ireland, British Transport Police Force, Ministry of Defence Police, Royal Navy Police, Royal Military Police, Royal Air Force Police, Security Service, Secret Intelligence Service, GCHQ, Ministry of Defence, Department of Health, Home Office, Ministry of Justice, National Crime Agency, Her Majesty's Revenue and Customs, Department for Transport, Department for Work and Pensions, Department for Work and Pensions, An ambulance trust in England, Common Services Agency for the Scottish Health Service, Competition and Markets Authority, Criminal Cases Review Commission, Department for Communities in Northern Ireland, Department for the Economy in Northern Ireland, Department of Justice in Northern Ireland, Financial Conduct Authority, A fire and rescue authority under the Fire and Rescue Services Act 2004, Food Standards Agency, Food Standards Scotland, Gambling Commission, Gangmasters and Labour Abuse Authority, Health and Safety Executive, Independent Police Complaints Commission, Information Commissioner, National Health Service Business Services Authority, Northern Ireland Ambulance Service Health and Social Care Trust, Northern Ireland Fire and Rescue Service Board, Northern Ireland Health and Social Care Regional Business Services Organisation, Office of Communications, Office of the Police Ombudsman for Northern Ireland, Police Investigations and Review Commissioner, Scottish Ambulance Service Board, Scottish Criminal Cases Review Commission, Serious Fraud Office and the Welsh Ambulance Services National Health Service Trust.
[259] Section 61(5)(b) of the IPA 2016.

(author's emphasis). The draft Communications Data Bill Joint Committee (dCDBJC) were satisfied with six[260] pubic authorities. [261] The dCDBJC also recommended that any public authority 'which make a convincing business case' should be listed on the statute.[262]It has not been made public, the business cases for the relevant public authorities, and when there has, it has not been satisfactory.[263] Chapter 6 also noted that the IPA 2016 was not clear if 'data' in s.61(2) meant communications data or the much broader definition found within s.263(1).

Section 61(4) allows officers to obtain data themselves from any *person* or telecommunications system,[264] ask *any person* whom is believed to be capable of obtaining communications data to do so,[265] and where they believe a telecommunications operator is *not already in* possession of but *maybe or is capable of obtaining any communications data*, by notice, require them to obtain data that is not already in their possession and disclose data subsequently obtained by them (author's emphasis).[266] This includes data that did not exist at the time of authorisation,[267] which could require telecommunications operators to generate and *retain* they may normally would not. Chapter 6 noted that 'public authorities may have broader powers of who they can obligate to retain than the Secretary of State' such as the 'IMSI-catchers' that can both track the movements of mobile phone users within a given area, and intercept texts and calls.[268]

It must be noted that said data can only be retained in specific investigations/operations,[269] and more worryingly for testing, maintaining or developing equipment, systems or *other capabilities* relating to the availability or obtaining of communications data.[270] Under both circumstances, massive amounts of communications data can be retained and masked due to the way in which items of communications data are recorded,[271] which may well strike the ECtHR as excessive in all aspects.[272] In dealing with the former, this still does not indicate what circumstances national security could be used as justification of said measure in specific investigations/operations. In dealing with the latter, there is no detailed indication as to what circumstances (reference to a specific investigation is an empty vessel) or when/how it would be necessary to conduct measures detailed in s.61(1)(b)(ii). The London Internet Exchange (LINX) in their written submissions to the draft Investigatory Powers Joint Bill Committee (dIPBJC) noted that it was 'not normally considered good practice to do systems development using live data: to reduce the risk of security breaches, *dummy data* is used (author's emphasis).'[273] They also noted that the use of data for the purpose of 'developing …other

[260] Police forces, National Crime Agency, Her Majesty's Revenue and Customs, the intelligence and security services, Financial Services Authority and the UK Border Agency.
[261] Joint Committee on the Draft Communications Data Bill, *Draft Communications Data Bill*, (2012-2013 HL 79 HC 479), para 128-9.
[262] ibid, para 137.
[263] For example, the Home Office maintained that simply because the Ministry of Defence could intercept communications, it should also be able to acquire communications data. Draft Investigatory Powers Joint Bill Committee, *written evidence*, (n43), Home Office, p500, para 40.
[264] Section 61(4)(a) of the IPA 2016.
[265] Section 61(4)(b) of the IPA 2016.
[266] Section 61(4)(c) of the IPA 2016.
[267] Section 61(5)(a) of the IPA 2016.
[268] Alon Aviram, 'Revealed: Bristol's police and mass mobile phone surveillance' (October 2016) <https://thebristolcable.org/2016/10/imsi/> accessed 16 July 2017.
[269] Section 61(1)(b)(i) of the IPA 2016.
[270] Section 61(1)(b)(ii) of the IPA 2016.
[271] '*30 days* of incoming and outgoing call data in relation to a mobile telephone would be counted as *one item of data*.' Report of the Interception of Communications Commissioner Annual Report for 2015 (HC 255 8 September 2016), para 7.23.
[272] *Iordachi*, (n219), [52].
[273] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n43), LINX, p918, para 45.

capabilities' would allow, under the guise of such development, analysis of data in ways that would not be authorised elsewhere.[274] Professor Lorna Woods also questioned *how* subjects will be chosen regarding testing capabilities.[275] The DSO's cannot be independent[276] and the fact that JC's approval is not required places any data retention obligations on the same arbitrary standing as the GC noted in *Zakharov* because there is no constraining power to limit under what circumstances said powers may be exercised.[277] Therefore, neither of these measures are foreseeable, and the latter is not even necessary.

Neither retention notices made by the Secretary of State and approved by the JC's or potential data retention obligations made by (un)authorised officers give any indication of the circumstances under which an individual's communications data (or data) may be retained on account of events or activities endangering national security. Therefore, it must be concluded that, due to the lack of definition of national security, no indication as to when national security may be invoked to issue a retention notice, the JC's judicial review process and the DSO's self-authorisation process not being a sufficient safeguard. Data retention obligations issued on even one telecommunications operator (or even in specific operations/investigations) cannot said to be foreseeable for the purposes of Article 8(2), because it grants unfettered powers to both JC's and DSO, does not indicate the scope of discretion conferred upon them, nor does it protect against arbitrary interference and is contrary to the rebuke of '*volenti nolenti* widespread, non-(reasonable) suspicion-based, "strategic surveillance" for the purposes of national security' established in *Zakharov*.[278] Therefore, even if EU law is not applicable in the national security context of retention, it would not pass the first ECHR hurdle.[279]

b. <u>for the purpose of preventing or detecting crime or of preventing disorder</u>

For the remainder of this subsection, the possible retention powers in s.61 will not be considered alongside powers in s.87. Where a violation is found, this will apply to equally to s.61.[280] In *Zakharov* the GC noted a specific list of offences is not necessary for foreseeability, but sufficient detail is required on the *nature* of the offences (author's emphasis).[281] In *Kennedy* the ECtHR accepted the UK's definition of 'serious crime' and its detection.[282] In the IPA 2016, serious crime[283] and its detection[284] has the same definition. However, the caveat when it comes to data retention, retention notices or possible retention via s.61 are not issued on the basis of 'serious crime,' just crime. Crime, nor disorder are defined in the IPA 2016. It has already been noted that the CJEU has held that *only* serious crimes could be used to justify data retention. The dCDBJC noted that '"[c]rime" can of course include trivial offences, and only the requirements of necessity and proportionality can prevent communications data being used

[274] ibid.
[275] ibid, p1387.
[276] Matthew White, (n4), 10.
[277] *Roman Zakharov*, (n6), [248-9].
[278] *Szabo*, (n152), Concurring Opinion of Judge Pinto de Albuquerque, [35].
[279] Council of Europe's Commissioner for Human Rights, (n197), para 20, p24. The Commissioner also recommended that national security should only be invoked relation to matters that threaten the very fabric and basic institutions of the nation, must be demonstrated that the threat cannot be met by means of ordinary criminal law, para 19, p24.
[280] As noted above, the rules for mass surveillance and individual surveillance are treated as the same even though the powers in s.61 do not refer to individual surveillance but specific investigations see *Liberty*, (n129), [63]; *Weber and Saravia v Germany* App no. 54934/00 (ECHR, 29 June 2000), [114].
[281] *Roman Zakharov*, (n6), [244].
[282] *Kennedy*, (n108), [34-5].
[283] Section 263(1) of the IPA 2016.
[284] Section 263(6) of the IPA 2016.

for such crimes.'[285] This is true, but this too would fall foul of being in accordance with the law as the ECtHR has noted concerns with laws that allow surveillance in 'respect of a very wide range of criminal offences'[286] as it would 'not provide adequate protection against abuse of power by the State.'[287] An example of abuse the ECtHR has noted is where 'the nature of the offences which may give rise to such an order are nowhere defined.'[288]

When justifying the dCDB to the dCDBJC, the Home Secretary said that the 'main purpose' was '[o]nly suspected terrorists, paedophiles or serious criminals will be investigated.'[289] This implies that it would not be the only purpose for data retention and its access, and given that the possibility to retain is possible by relevant public authorities via s.61 of the IPA 2016, it is of concern that the National Police Chiefs' Council lead on digital crime, Stephen Kavanagh said officers should sometimes 'push the boundaries' and sometimes 'go beyond what the regulations or courts accept' to protect the public.[290] This adds to the conclusion that a lack of definition of crime and disorder makes retention notices unforeseeable as there is no indication as to what circumstances data retention is permissible.

One would go further in agreeance with Judge Pinto de Albuquerque in *Szabo* where he noted that:

> I cannot share the Chamber's statement that "the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions *listing in detail all situations that may prompt a decision to launch secret surveillance operations*"…which not only *downgrades the role of the principle of legality in a field of law where its rigorous reading is most needed*, but *also leaves the door wide open to creative interpretation of the law by Government and therefore to State abuse* (author's emphasis).[291]

An exhaustive list of offences for the purposes of data retention was also the position of the GFCC,[292] EU's Article 29 Working Party (WP29)[293] and was accepted by the ECtHR's (among other safeguards) admissibility in *Weber and Saravia*[294] as containing the *minimum* safeguards against arbitrary interference.[295] Given that in the *Szabo* the ECtHR called for more acute protection of Article 8 in the era of mass surveillance,[296] such an addition would be welcome and consistent with the requirements for foreseeability in this context.

c. in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security

[285] Joint Committee on the Draft Communications Data Bill, (n261), para 141.
[286] *Roman Zakharov*, (n6), [244]; *Iordachi*, (n219), [44].
[287] *Iordachi*, (n219), [53].
[288] *Kruslin v France* App no. 11801/85 (ECHR, 24 April 1990), [35].
[289] Joint Committee on the Draft Communications Data Bill, (n261), para 141.
[290] Martin Bentham, 'Police 'must be given power to shut websites in child abuse and revenge porn fight'' *The Standard* (16 December 2016) <http://www.standard.co.uk/news/crime/police-must-be-given-power-to-shut-websites-in-child-abuse-and-revenge-porn-fight-a3422131.html> accessed 17 July 2017.
[291] *Szabo*, (n152), Concurring Opinion of Judge Pinto de Albuquerque, [17], n31.
[292] BVerfG, (n176), [228].
[293] Article 29 Working Party, 'Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector' (27 February 2014) < http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf> accessed 22 August 2017, para 6.1.
[294] *Weber and Saravia*, (n280), [96],
[295] ibid, [101].
[296] *Szabo*, (n152), [53].

Like national security and crime, 'economic well-being' is not defined in the IPA 2016. Nor is there any indication as to what 'relevant to the interests of national security' means. The JCDIPB noted that witnesses felt the term was too vague.[297] Professor John Naughton and Professor David Vincent suggested that it was appropriate that the term receive critical scrutiny by Parliament.[298] Lord Carlise, although against a statutory definition called for 'greater understanding' for clarity on the process of certification and who is involved.[299] The JCDIPB recommended a statutory definition of 'economic well-being.'[300] Days later, the Intelligence and Security Committee (ISC) noted that the term was unnecessarily confusing and complicated.[301] They continued that it is also redundant because it is a subset of national security.[302] Worryingly, when the ISC questioned the intelligence agencies and the Home Office 'neither [had] provided any sensible explanation'[303] for its inclusion. The ISC recommended that 'economic well-being' be removed altogether from the legislation.[304] Baroness Jones also sought to clarify 'economic well-being' because the core purposes for which extraordinary powers may be used remain undefined and dangerously flexible.[305] Jones continued that:

> [T]he undefined tests of…economic well-being risk interference with political and other lawful activity that ought to be unimpeded in a democratic society. In an era when parliamentarians from both Houses have been subjected to inappropriate surveillance by security services and the police, the continued undefined use of these terms in enabling legislation is not appropriate or sustainable.[306]

Vague terminology such as 'economic well-being' does not indicate the circumstances in which retention via Part 4 or Part 3 would be used, and thus also does not satisfy the foreseeable requirement.

d. <u>in the interests of public safety and for the purpose of protecting public health</u>

These two grounds are dealt with together due to their vagueness leading to the same result. In *Iordachi* the ECtHR noted that:

> [I]t is *unclear* under the impugned legislation *who – and under what circumstances – risks having the measure applied to him or her in the interests of, for instance, protection of health or morals or in the interests of others*. [Moldovan law] fails, nevertheless, to *define* "national security", "public order", *"protection of health"*, "protection of morals", "protection of the rights and interests of others", "interests of ... the economic situation of the country" or "maintenance of legal order" for the purposes of interception of telephone communications. Nor does the legislation specify the

[297] Joint Committee on the Draft Investigatory Powers Bill, (n45), para 693.
[298] ibid.
[299] ibid, para 694.
[300] ibid, para 696.
[301] Intelligence and Security Committee, *Report on the draft Investigatory Powers Bill*, (2016, HC 795), para J(i).
[302] ibid.
[303] ibid.
[304] ibid.
[305] HL Deb 12 September 2016, (n227), col 1315.
[306] ibid, col 1351-1316.

> circumstances in which an individual may be at risk of having his telephone communications intercepted on any of those grounds (author's emphasis).[307]

This clearly indicates that the ECtHR does not accept a simple reference to the qualified aspects of Convention Rights as justification for interference. In *Doerga v Netherlands* the Government argued that tapping and retention of conversations[308] were justified on the grounds of public safety and the protection of the rights and freedoms of others.[309] However, when examining the law under 'foreseeability,'[310] the ECtHR noted they lacked both clarity and detail nor did it 'give any precise indication as to the circumstances in which prisoners' telephone conversations may be monitored, recorded and retained or the procedures to be observed.'[311] The ECtHR concluded that this was not 'in accordance with the law'[312] and therefore demonstrates reliance on a specified qualified ground in and of itself will fall foul of the ECtHR's standard of legality.

e. Other purposes

The remaining purposes for retention are dealt with together under this subsection. Reasons for retention notices set out in s.61(7)(g)-(i) deal with specific instances. It is not clear how the retention of communications data would prevent death/injury/damage to a person's physical/mental health as data preservation would be more suited to deal with such immediate situations. Moreover, the fact that this specific circumstance can elicit the retention of data on a massive scale (any or all data, from one[313] or all telecommunications operators) renders a well-intentioned reason for retention indiscriminately[314] arbitrary[315] and thus not satisfying foreseeability for creating an unfettered and arbitrary power. Similarly, with identifying a person, such a power can impose retention of data arbitrarily and indiscriminately, thus lacking foreseeability. With regards to miscarriages of justice, it is not clear what miscarriages of justice entail and under what circumstances a retention notice may be issued on those grounds, therefore, again, not foreseeable.

Sections 61(7)(f) like with most reasons for a retention notice does not indicate under what circumstances a retention notice could be issued for assessing or collecting tax/duty/levy etc. This provision also becomes arbitrary and indiscriminate because of the amount of data that could be retained on the off chance that *someone* may owe the government money. Finally, s.61(7)(j) too does not indicate under what circumstances retention is permissible for the regulation of financial services and markets. It is also not indicated what 'functions' exercised are relevant for the retention of communications data. Moreover, is also not clear on what is meant by functions relating to financial stability i.e. for whom or what? Is this synonymous with 'economic well-being' as a standalone justification? In *Iordachi*, it was already noted that the 'interests of the economic situation of the country' was too vague, so too is financial stability. This renders both provisions unforeseeable for the purposes of legality and are therefore nor 'in accordance with the law.'

---

[307] *Iordachi*, (n219), [46].
[308] *Doerga v Netherlands* App no. 50210/99 (ECHR, 27 April 2004), [43].
[309] ibid, [36].
[310] ibid, [50].
[311] ibid, [52].
[312] ibid, [54].
[313] Andrew D. Murray, (n165), 161.
[314] *Kennedy*, (n108), [162].
[315] *Roman Zakharov*, (n6), [302].

ii. Persons liable

a. A failure to distinguish between suspects and non-suspects

> What makes a law foreseeable is the extent to which it distinguishes between different classes of people, thereby placing a limit on arbitrary enforcement by the authorities.[316]

Although *S and Marper* concerned the retention of DNA/fingerprint data, it still has clear applications to communications data retention.[317] The GC criticised the UK regime for not distinguishing between those who had been *suspected* and those who had committed offences.[318] Data retention in the IPA 2016 does not distinguish between those who have committed offences, those who are suspects, and those who are not suspects at all. This is problematic for foreseeability purposes. The GC in *Zakharov* noted that the authorisation authority's (JC's) scope of review must be capable of verifying:

> [T]he existence of a *reasonable suspicion* against the *person* concerned, in particular, whether there are *factual indications* for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security (author's emphasis).[319]

Not only that, the GC noted that, even if reasonable suspicion has been verified, the authorisation of a surveillance measure should only occur 'if it meets the requirements of necessity and proportionality.'[320] This criminal activity and reasons for authorisation must be serious,[321] which would be consistent with the Council of Europe's (CoE) Committee of Ministers (CoM) Recommendation Rec(2005)10 Chapter II(b)(4).[322] Said ECHR principles applies to targeted or generalised surveillance.[323] Given that the ECtHR has transferred principles of independence from its interpretation of 'officer' in Article 5(3) into the surveillance context, 'reasonable suspicion' found within Article 5(1)(c) is also transferable.[324] Reasonable suspicion requires the circumstances mitigating for and against a measure, deciding

---

[316] Abu Bakar Munir and Siti Hajar Mohd Yasin, (n173), 755.
[317] Ian Brown, 'Communications Data Retention in an Evolving Internet' (2010) International Journal of Law and Information Technology 19:2 95, 103.
[318] Matthew White, (n4), 35.
[319] *Roman Zakharov*, (n6), [260].
[320] ibid, [262].
[321] *Iordachi*, (n219), [51].
[322] Recommendation Rec(2005)10 of the Committee of Ministers to member states on "special investigation techniques" in relation to serious crimes including acts of terrorism, 20 April 2005.
[323] *Liberty*, (n129), [63]; *Weber and Saravia*, (n280), [114]. It must be noted that data retention in the IPA 2016 must be distinguished from the surveillances measures in *Weber and Saravia*. Firstly, 'strategic monitoring' concerned 6 specific offences in which interception could be ordered [96]. Secondly, 'strategic monitoring' only concerned international calls (mostly via satellite, ~ 10% of communications [30], [110]) where specific catchphrases that were capable of triggering an investigation into those specific offences or had be foreign nationals or companies whose telephone connections could be monitored deliberately in order to avoid such dangers [97]. This distinguishing feature is also highlighted by Judge's Koskelo and Turković in *Big Brother Watch v UK* App nos. 58170/13, 62322/14 and 24960/15 (ECHR, 13 Septemeber 2018), where they note that 'in Weber and Saravia, carried over to a surveillance regime which did have more similarities with the RIPA section 8(4) regime but *nevertheless operated in conditions very different from those prevailing in the modern digitalised societies*' [29]. In any event judge Pinto de Albuquerque noted the *Roman Zakharov* marked a rebuttal of 'strategic surveillance' (*Szabo*, (n152), Concurring Opinion of judge Pinto de Albuquerque, [35]).
[324] Matthew, (n4), 5, 35.

by reference to legal criteria whether the reasons justify the measure,[325] in other words a consideration of the *merits* of the decision.[326] When the requirements of reasonable suspicion are not met, or the measure is unlawful, the measure must stop.[327] Reasonable suspicion requires more than suspicion held in good faith, it 'requires the existence of facts or information which would satisfy an objective observer that the person concerned may have committed the offence' which is dependent in all the circumstances.[328] This threshold is higher than the 'identifiable public' the CJEU eluded to in *Tele2 and Watson* as suspicion would not be necessary for data retention.[329] Most data retained will be of individuals who bear no relation to serious crime and therefore such retention of data is clearly irrelevant.[330] Even prior to the CJEU's position in *Tele2 and Watson*, AG Kokott in *Promusicae* doubted whether the *storage of traffic data of all users without any concrete suspicions*, laying in a stock, is compatible with fundamental rights (author's emphasis).[331]

Data retention all but eliminates any prospect of reasonable suspicion being applied. Judge Pinto de Albuquerque noted that any watering down of reasonable suspicion assumes that the fight against terrorism requires a:

> [P]ool of information retrievable by the authorities applying highly efficient methods and processing masses of data, potentially about each person, should he be, one way or another, connected to suspected subjects or objects of planned terrorist attacks.[332]

As noted in section 7.4(B)(1)), data retention affects those *irrespective of conduct*, *almost exclusively* affects persons who do not give rise to a cause for it, *nor will they ever be connected* in any way to serious crime. Tom Sorell highlights that there is no reason to think most of the population is contemplating criminal activity.[333] Suspicionless searches, as Daniel Solove contends, provides law-enforcement officials with too much power and discretion and little oversight.'[334] Judge Pettiti in *Kopp v Switzerland*[335] noted that surveillance 'must be used *for a specific purpose*, *not as a general "fishing"*'[336] exercise to bring in information (author's emphasis).' Fishing has been likened to data retention as individuals are not targeted.[337]

Milaj and Bonnici note that mass surveillance is more intrusive than targeted since they interfere largely with the life of innocent individuals, devoid of any suspicion, only on the basis

[325] *Pantea v Romania* App no. 33343/96 (ECHR, 3 June 2003), [231].
[326] *Aquilina v Malta* App no. 25642/94 (ECHR, 29 April 1999), [47].
[327] *McKay v the United Kingdom* App no. 543/03 (ECHR, 3 October 2006), [40].
[328] *Ilgar Mammadov v Azerbaijan* App no. 15172/13 (ECHR, 22 May 2014), [88]; Matthew White, (n4), 35.
[329] Matthew White, (n4), 35.
[330] ibid.
[331] Case C‑275/06 *Promusicae v Telefónica de España SAU* [2007] ECR I-00271, Opinion of Kokott, [82].
[332] *Szabo*, (n152), Concurring Opinion of Judge Pinto de Albuquerque, [20].
[333] Tom Sorell, 'Preventive policing, surveillance, and European counter-terrorism' (2011), Criminal Justice Ethics 30:1, 1.
[334] Daniel Solove, *Nothing to Hide. The False Trade off between Privacy and Security* (Yale University Press 2011), 17.
[335] *Kopp*, (n158).
[336] Stephen Uglow, 'The Human Rights Act 1998: Part 4: covert surveillance and the European Convention on Human Rights' [1999] Criminal Law Review 287, 289.
[337] Franziska Boehm and Paul de Hert, *The rights of notification after surveillance is over: ready for recognition?* (Yearbook of the Digital Enlightenment Forum, IOS Press 2012), pp. 19-39; Matthew White, (n4), 39.

of making use of certain ways of communication or of certain devices.[338] One would go further and argue that the requirement of verifying reasonable suspicion is not and cannot be addressed because it is not based on individual actions, or even group actions, but on service used,[339] a point also noted by the GFCC.[340] Applying judicial review principles would not remedy the absence of proving reasonable suspicion,[341] and thus would not curb wide powers 'to offer the individual adequate protection against arbitrary interference.'[342] The failure to define sufficiently clearly the categories of persons liable for surveillance would concern the ECtHR[343] which would lack foreseeability.[344] As the CoE's Commissioner HR noted that 'suspicionless *mass retention* of communications data is fundamentally contrary to the rule of law.'[345]

b. When a person who is not a suspect but may have information for a derogation purpose

In *Zakharov* the GC reiterated that 'interception measures in respect of a person who was not suspected of any offence but could possess information about such an offence might be justified under Article 8.'[346] However, this requires the offences and persons liable to be sufficiently clear,[347] which if not (as is the case with regards to Part 4) can lead to a violation.[348]

c. A failure to make provisions for special categories of communications

Privacy International noted that:

> Blanket data retention laws also offend the principle of foreseeability because they make no distinction for relationships that the State already recognises as sufficiently special to warrant a degree of protection.[349]

The interference with lawyer-client privilege posed by data retention was highlighted in Chapter 4. The absence of protections for (not just lawyer-client privilege) in the data retention context was highlighted by the CJEU[350] and AG Saugmandsgaard Øe who noted it would be desirable to exclude said data from retention obligations.[351] In *Iordachi*, the ECtHR were 'struck by the absence of clear rules defining what should happen when, for example, a phone call made by a client to his lawyer is intercepted.'[352] In *Kopp* the ECtHR found Swiss law to fail foreseeability because it provided 'no guidance on how authorities should distinguish

[338] Jonida Milaj and Jeanne Pia Mifsud Bonnici, 'Unwitting subjects of surveillance and the presumption of innocence' (2014) Computer Law and Security Review 30:4 419, 423.
[339] Matthew White, (n4), 41.
[340] BVerfG, (n176), [177].
[341] *Gillan Quinton v UK* App no. 4158/05 (ECHR, 12 January 2010, [86]; *Beghal*, (n168), [98].
[342] ibid, [79].
[343] *Iordachi*, (n219), [44].
[344] Abu Bakar Munir and Siti Hajar Mohd Yasin, (n173), 755. Though *Kruslin*, (n288), [35] and *Huvig v France* App no. 11105/84 (ECHR, 24 April 1990), [34] highlighted more than just lack of clarification on persons liable.
[345] Council of Europe's Commissioner for Human Rights, (n197), para 6, p22.
[346] *Roman Zakharov*, (n6), [245]; *Greuter v the Netherlands* App no. 40045/98 (ECHR, 19 March 2002).
[347] *Roman Zakharov*, (n6), [245]; *Iordachi*, (n219), [44].
[348] *Kruslin*, (n288), [35-36]; *Amann*, (n126), [60], [62].
[349] Privacy International, (n141), p9.
[350] *Digital Rights Ireland and Seitlinger and Others*, (n2), [57-8]; *Tele2 Sverige AB and Watson*, (n3), [105].
[351] Opinion of Saugmandsgaard Øe, (n1), [212].
[352] *Iordachi*, (n219), [50].

between protected and unprotected attorney-client communications.'[353] Data retention in Part 4 suffers from the same flaw because they 'make no effort to distinguish between such communications (and others like it) and "normal" communications.'[354]With regards to journalistic sources, the ECtHR defines it as:

> "any person who provides information to a journalist"; it understands "*information identifying a source*" to include, as far as they are *likely to lead to the identification of a source*, both "*the factual circumstances of acquiring information from a source by a journalist*" and "the unpublished content of the information provided by a source to a journalist (author's emphasis)."[355]

Due to the failure to make laws specifically for journalistic sources, though acceptable in *Weber*[356] the ECtHR noted that one cannot restore the confidentiality of journalistic sources once it has been destroyed.[357]

Subsection 7.4(B)(2)(i)) has demonstrated that where persons liable for surveillance measures and of the nature of offences for surveillance measures are not defined, this fails foreseeability. This is the case in either the former, or latter, or when both are considered together.[358] Privacy International have argued that data retention laws that fail to distinguish between different classes of people would have a more pernicious impact on individual privacy than the vague laws at issue in *Kruslin* and *Amann*.[359]

iii. Incidental Data Retention

This relates particularly to the correspondence aspect of Article 8. As the RCC noted, data retention unjustly restrains the privacy of the *recipient* as the person becomes exposed to data retention *irrespective* of their own act, but based on the behaviour of another person.[360] This exposes them to bad faith and blackmail.[361] The RCC also pointed out that this makes passive subjects of communications suspects from the point of view of the authorities, which was regarded as an excessive intrusion into their private life.[362]Thus, in the RCC's view, was excessive.[363] In *Kruslin*, the case actually concerned the incidental interception[364] of the applicant's communications. Due to there being a lack of clarity on the persons liable nor nature of offences defined, the French law was not 'in accordance with the law.'[365] Part 4 of the IPA 2016 suffers from the issue of incidental data retention, and would too similarly violate the ECHR.

---

[353] Privacy International, (n141), p9; *Kopp*, (n157), [73-75].
[354] Privacy International, (n141), p9.
[355] *Telegraaf and Others*, (n121), [86].
[356] *Weber and Saravia*, (n280), [151]. The ECtHR's reasoning was based on due to 'strategic monitoring' was not aimed at identifying journalistic sources, the interference was not as serious. However, it is contended whether or not an intrusive measure is directed at everyone, or a particular class of people, the seriousness of that interference is not reduced. If anything, the seriousness increases because there is a weaker (or non-existent) justification for said interference. See also distcintion made in (n232).
[357] *Telegraaf and Others*, (n121), [101].
[358] *Kruslin*, (n288), [35-36]; *Amann*, (n126), [60], [62].
[359] Privacy International, (n141), p9.
[360] Romania Constitutional Court, (n148).
[361] ibid.
[362] ibid.
[363] ibid.
[364] *Kruslin*, (n288), [25-6].
[365] ibid, [36].

iv. Data by type

It was already noted above that a requirement for foreseeability was to have *clear* binding rules especially in light of the sophistication of modern technology. Data retention is a unique surveillance power in which it can detail what data is to be retained. Chapter 3 detailed the types of communications data that is likely to be retained. The RCC noted 'that the lack of a precise legal provision that will exactly determine the sphere of the data necessary to identify physical and legal users, opens up the possibility for abuses in the activity of retaining.'[366] Chapter 3 noted the problems of obliging telecommunications operators to *generate* data because it allows for undefined types of data to be retained. It also noted that it is possible to oblige telecommunications operators to oblige third parties to generate and hand over communications data. Even with regards to ICRs (which the IPA 2016 does not limit itself to), the Home Office noted that 'there is no single set of data that constitutes an internet connection record.'[367] Then with regards to smart objects (to which retention notices can be applied to), they can accumulate a massive amount of data[368] which the nature of such traffic are *currently unknown*.[369] Even with explanatory notes, the IPA 2016 does not account for the types of data that can be generated, admits that ICR lacks precision and with the IoT, there is a void in what types of data that can be created (and subsequently retained). Chapter 3 also highlighted that Big Data could be retained in various possible ways via generation, entity data retention, and retaining any/all descriptions of data. There is also the fact that the IPA 2016 does not explicitly rule out data for the purposes of s.263(1) not falling within the ambit communications data which allows nigh unlimited amounts of types of data to be retained. The JCDIPB recommended that the government clarify the types of data it expects CSPs to generate and in what quantities so that this information can be considered when the Bill is introduced.[370] This did not occur. Moreover, Chapter 3 highlighted that telecommunications operators could subsequently retain third party data because they were permitted to conduct interception for non-defined 'business activities.' Finally, Chapter 3 noted that content can be retained that is imbedded within communications data. Therefore, in this regard, the rules on the types of data to be retained are not sufficiently clear and thus, not foreseeable.

C. Utility

Lord Kerr in *Beghal* noted that even if the utility of a measure is demonstrated, it would be 'misconceived' to assume it 'meets the requirement that the measure be "in accordance with law."'[371] This is especially so when the powers (as demonstrated above and will do so below) are used in an arbitrary or discriminatory manner.[372] Therefore, even if the utility (discussed below) is sufficiently proven, the fact remains, data retention as currently envisioned in the IPA 2016, does not meet the requirements of being 'in accordance with the law' because it is inherently general and indiscriminate.

D. A violation of Article 8 is a violation of Articles 9-11 and Article 2 Protocol 4

[366] Romania Constitutional Court, (n148).
[367] Communications Data: Draft Code of Practice – Home Office, 1 March 2016, p.18.
[368] Friedemann Mattern and Christian Floerkemeier, 'From the Internet of Computers to the Internet of Things' <http://vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf> accessed 25 July 2017, p15.
[369] Luigi Atzori, Antonio Iera and Giacomo Morabito, 'The Internet of Things: A survey, Computer Networks' (2010) 54:15 2787, 2800.
[370] Joint Committee on the Draft Investigatory Powers Bill, (n45), para 209.
[371] *Beghal*, (n168), [107].
[372] ibid, [93].

Section 7.4 noted that prescribed by/in accordance with the law were to be treated as the same for the purposes of Articles 8-11 and Article 2 Protocol 4. Although Article 2 Protocol 4 has not been ratified by the UK or incorporated through the HRA 1998, it can be used to inform Article 8,[373] due to the collection of data concerning movement interferes with Article 8.[374] This discussion is also important for Member States that *have* incorporated Article 2 Protocol 4. *Segerstedt-Wiberg and Others v Sweden*[375] concerned the storage of information (retention) by the Security Police.[376] After finding a violation of Article 8[377] it was further argued due to their political affiliations Articles 10 and 11 were also violated.[378] Even though the ECtHR noted that the applicants did not deduce any evidence of a chilling effect on their political freedoms it nevertheless considered that:

> [T]he *storage* of personal data *related to political opinion, affiliations and activities* that is deemed *unjustified for the purposes of Article 8 § 2 ipso facto constitutes an unjustified interference with* the rights protected by *Articles 10 and 11* (author's emphasis).[379]

This demonstrates that any measure in the surveillance context which violates Article 8, which engages Articles 10 and 11 for the same reason, also violates those Articles, *even when the severity of the interference cannot be demonstrated*. In addition, communications data potentially allows the storage of personal data which relates to one's movements (Article 2 Protocol 4) and religious beliefs (Article 9) and similarly with Articles 10-11, this would amount to violations for not being 'in accordance with the law.'

E. Conclusions

This subsection has demonstrated that had the CJEU not skipped the legality requirement, observed AG Saugmandsgaard Øe's request for clarification[380] and followed ECtHR jurisprudence faithfully, whether it be on the basis of an unfettered arbitrary power, or strict surveillance requirements set out in the ECtHR's case-law, the assessment of proportionality would not have been necessary. Although the position of the ECtHR when finding a measure not to be 'in accordance with the law' is sometimes to discontinue its assessment, the ECtHR can *still* consider whether the measure pursued a legitimate aim and was proportionate.[381]

7.5 Does data retention pursue a Legitimate aim?

A legitimate aim is the list of exceptions[382] found within a Convention Right i.e. national security. Such exceptions are exhaustive and their definition is restrictive, and for a

[373] Matthew White, 'When can EU citizens be expelled from the UK after Brexit? The Human Rights Dimension' (4 October 2016) <https://eulawanalysis.blogspot.co.uk/2016/10/when-can-eu-citizens-be-expelled-from.html> accessed 15 March 2018.
[374] *Uzun*, (n140), [51-53]; *Shimovolos*, (n131), [72].
[375] *Segerstedt-Wiberg and Others v Sweden* App no. 62332/00 (ECHR, 6 June 2006).
[376] ibid, [70].
[377] ibid, [92].
[378] ibid, [105].
[379] ibid, [107].
[380] Opinion of Saugmandsgaard Øe, (n1), [137].
[381] *Kurić and others*, (n138), [350].
[382] *Biržietis v Lithuania* App no. 49304/09 (ECHR, 14 June 2016), [53].

qualification to be compatible with the ECHR, it must pursue an aim 'that can be linked to one of those listed in that provision.'[383] In *S and Marper* the GC agreed that DNA/fingerprint retention pursued the legitimate aim of detection/prevention of crime.[384] Gerards notes that the ECtHR usually accepts very general and abstract aims such as national security, it however, adds very little to its reasoning.[385] However, Judge Wildhaber's *et al's*[386] concurring opinion in *Rotaru v Romania* stressed that:

> [I]n respect of *national security as in respect of other purposes*, there has to be *at least* a *reasonable and genuine link between the aim invoked and the measures interfering with private life for the aim to be regarded as legitimate. To refer to the more or less indiscriminate storing* of information relating to the private lives of individuals in terms of pursuing a legitimate national security concern *is ... evidently problematic* (author's emphasis).[387]

Although the case concerned the continued storage of information for decades, the judges continued that the ECtHR were entitled to find that the measure did not pursue a legitimate aim. It is also important to note that the concurring judges did not confine this point to national security, but all the limitations set out in Article 8, therefore, the same logic applies. Moreover, as Chapter 3 noted, algorithms, profiling and data mining techniques could be utilised in retention notices or to retain data that has been subject to such techniques. The Consultative Committee of the Convention for the Protection of Individuals Data with regards to Automatic Processing of Personal Data noted that any dynamic-algorithmic-based data mining and profiling for predictive or preventative policing is not a legitimate aim in a democratic society.[388] They continued that any bulk data on general populations for data-mining and profiling should also be rejected.[389]

There is but another problem with regards to data retention in pursuit of a legitimate aim, the grounds themselves. Although it was highlighted that 'in accordance with the law' and 'prescribed by law' meant the same thing, this does not ring true for the actual derogations in Articles 8-11 and Article 2 Protocol 4. For example, Articles 8, 10, 11 and Article 2 Protocol 4 all allow restrictions in the interests of national security. However, because there is no national security exemption in Article 9, '[s]tates may therefore not interfere with that right on that ground.'[390] This was highlighted by the ECtHR in *Nolan and K v Russia* where it was noted that:

> Far from being an accidental omission, the non-inclusion of that particular ground for limitations in Article 9 reflects the primordial importance of religious pluralism as "one

---

[383] ibid.
[384] *S and Marper*, (n107), [100].
[385] Janneke Gerards, 'How to improve the necessity test of the European Court of Human Rights' (2013) I•CON 11:2 466, 479-480.
[386] Judges Makarczyk, Türmen, Costa, Tulkens, Casadevall, Weber and Lorenzen in a separate concurring opinion.
[387] *Rotaru v Romania App no. 28341/95 (ECHR, 4 May 2000).*
[388] Douwe Korff, 'Passenger Name Records, data mining & data protection: the need for strong safeguards' (15 June 2015) <https://rm.coe.int/16806a601b> accessed 15 March 2018, p107.
[389] ibid.
[390] Douwe Korff, 'The Standard Approach Under Articles 8-11 ECHR and Article 2 ECHR' (2009) <http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf> accessed 26 July 2017; Guide to Article 9, (2015) <http://www.echr.coe.int/Documents/Guide_Art_9_ENG.pdf> accessed 26 July 2017, para 31.

> of the foundations of a 'democratic society' within the meaning of the Convention"...It follows that the interests of national security could not serve as a justification for the measures taken by the Russian authorities...[391]

As Breyer suggests, even when rights are partially identical, they have different purposes and therefore need to be applied independently of each other.[392] When retention notices are issued in the interests of national security, this becomes problematic due to the interference with Article 9. Blanket data retention whether by one or multiple telecommunications operators makes it impossible to distinguish between interferences with Article 8, 9, 10, 11 and Article 2 Protocol 4, hence why Chapter 4 argued they were all engaged. Therefore, the only way to ensure Article 9 is respected and/or to prevent any incidental interference, data retention on national security grounds must not be permitted. Out of the five Convention Rights mentioned, it is only Article 8 that refers to 'economic well-being' and therefore, retention notices on this ground are not permissible for the rest. Public order is a derogation that is not permissible under Article 8, but is for Article 9 and Article 2 Protocol 4.

Furthermore, to confine a legitimate aim to what is mentioned in the derogations of qualified rights prevents the ECtHR from distinguishing between various aims.[393] This is not desirable as the easy acceptance of broad terms which are mostly empty and meaningless in character has the result of that the requirement of a legitimate aim does not add anything substantial to the judicial reasoning in cases of conflicts between rights or interests.[394] When the margin of appreciation is narrowed the Court should be more precise than it currently appears to be in determining the interests served by the measure.[395] This demonstrates just as Judge Wildhaber's *et al's* and the other judges noted in *Rotaru*, the more or less indiscriminate storing of personal information makes any legitimate aim problematic. This needs to be seriously considered in order for the Convention to be practical and effective, and not theoretical and illusory,[396] as a failure to establish a legitimate aim will result in a violation.[397] This also highlights an example where the ECHR is narrower with regards to exemptions to qualified rights as the CFR only requires satisfying the general interest.

7.6 Is data retention necessary in a democratic society?

As the Institute for Prospective Technological Studies noted privacy could regain something of its esteem if the ECtHR would stop to focus only upon the legality criterion and start again taking the necessity test seriously.[398] The GC did just that in *Zakharov* in which 'in accordance

---

[391] *Nolan and K v Russia* App no. 2512/04 (ECHR, 12 February 2009), [73].
[392] Patrick Breyer, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR' (2005) European Law Journal 11:3 365, 373; Stephen Greer, 'The Margin of Appreciation: Interpretation and Discretion under the European Convention on Human Rights' (2000) <https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17(2000).pdf> accessed 2 March 2018.
[393] Janneke Gerards, (n385), 479.
[394] ibid, 480.
[395] ibid, 481.
[396] *Roman Zakharov*, (n6), [288].
[397] *Erményi v Hungary* App no. 22254/14 (ECHR, 22 November 2016), [37-40]; *Khuzhin and Others v Russia* App no. 13470/02 (ECHR, 23 October 2008), [117-118]; *Rotaru, (n387), Concurring Opinions of* Judge Wildhaber's *et al*.
[398] Institute For Prospective Technological Studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*: Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs, European Communities (2003) <http://ftp.jrc.es/EURdoc/eur20823en.pdf> accessed 12 August 2017, p147.

with the law' and 'necessary in a democratic society' were considered jointly.[399] Judge Pinto de Albuquerque in his concurring opinion in *Szabo* noted that mandatory data retention 'appears neither necessary nor proportionate.'[400] This section will highlight why this is correct.

A. Pressing Social Need

> [T]he term 'pressing social need' implies *a greater level of severity, urgency or immediacy* associated with the need that the measure is seeking to address (author's emphasis).[401]

a. Necessity

'Necessary,' the ECtHR has asserted, is not synonymous with "indispensable" but it also did not have the flexibility of an expression such as 'admissible,' 'ordinary,' 'useful,' 'reasonable' or 'desirable.'[402] It is not sufficient to establish the utility of a measure, thus '[t]he onus upon the public authority seems to be significantly higher.'[403] This onus intensifies further given that data retention significantly interfere with wide spectrum of human rights.[404] 'Necessity' relates not just to a measure applying the law, but the law itself.[405]

The Joint Committee on Human Rights (JCHR) have opined that '[t]here must be a sufficient factual basis for believing that there was a real danger to the interest which the State claims there was a pressing social need to protect.'[406] The necessity requirement will subdivide into four components, whether there was a pressing social need for the definition of telecommunications operators to be extended, for the type of retention itself, the retention length, and the inclusion of ICRs, all the other types of data and the ability to *generate* data.

i. Is there a pressing social need for retention obligations to encompass everything that can communicate?

Chapter 6 demonstrated that retention obligations could be imposed on essentially any service, system, device etc that communicates, and on any person, organisation, entity that controls said services/systems/devices. Chapter 6 noted, this increases the severity of the interference further in light of the IoT, in which many aspects of a person's home would be their own personal Panopticon. It could be argued to be justified on the basis of the increase in use and in diversity of technology, as such, a broad and technologically neutral definition was appropriate as means of future-proofing the law.[407] However, Smith highlighted that the JCDIPB did not explicitly address 'whether a case for extension to private networks (as opposed to smaller public networks) has been made out.'[408] Smith continues that the Home Office made no attempts 'to

---

[399] *Roman Zakharov*, (n6), [236].
[400] *Szabo*, (n152), Concurring Opinion of Judge Pinto de Albuquerque, [6].
[401] Article 29 Working Party, (n293), para 3.14.
[402] *Handyside v United Kingdom* App no. 5493/72 (ECHR, 7 December 1976), [48].
[403] *Pullen & Ors -v- Dublin City Council* [2008] IEHC 379, [12(c)].
[404] Paul Bernal, (n42), 259.
[405] *Handyside*, (n402), [49].
[406] Joint Committee on Human Rights, (n123).
[407] Graham Smith, 'Future-proofing the Investigatory Powers Bill' (15 April 2016) <http://www.cyberleagle.com/2016/04/> accessed 5 March 2018.
[408] Graham Smith, 'The draft Investigatory Powers Bill - start all over again?' (16 February 2016) <http://www.cyberleagle.com/2016/02/the-draft-investigatory-powers-bill.html> accessed 27 July 2017.

justify the extension to all private networks.'[409] Smith concluded with an important question, that remains unanswered: If there is no intention to use the powers against private networks, why are the powers that broad? If it is intended, *where is the justification*?[410] There is a lack of consideration into how the definition includes IoT services/devices etc let alone justification. It is this lack of consideration and justification which renders the pressing social need in this regard non-existent. As the ACC noted 'mere possibility of using new technology in addition to existing surveillance measures does not *a priori* justify an interference.'[411] Failing on the grounds of establishing a pressing social need will in itself amount to a violation,[412] and would thus violate all the relevant rights mentioned above.

ii. Is there a pressing social need for retention in its current form?

The justification for the IPA 2016's necessity[413] under the ECHR is derived from the case of *K.U. v Finland*.[414] This concerned Finland's inability to obtain the identity of a person who subjected a minor to advertisements of a sexual nature,[415] which lead to a violation of Article 8.[416] The ECtHR referred to the State's positive obligation under Article 8[417] to criminalise offences and attempts against a person and to 'reinforce the deterrent effect of criminalisation by applying criminal-law provisions in practice through effective investigation and prosecution' with even greater importance when it concerns children.[418] The ECtHR noted that:

> Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield *on occasion* to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others (author's emphasis).[419]

Such a positive obligation is also prevalent in the wording of Article 2 (right to life) by requiring everyone's life to be protected by law and also in the jurisprudence of the ECtHR with regards to effective criminal law provisions,[420] whether the State is directly involved.[421] This also includes effective official investigations.[422] However, in *K.U.* the ECtHR also noted that Article 8 and 10 must yield *on occasion*[423] to imperatives, such as effective criminal laws. Moreover, with regards to positive obligations for effective criminal laws/investigations, the ECtHR has noted:

---

[409] ibid.
[410] ibid.
[411] Austrian Constitutional Court, (n175), [2.3.14.1].
[412] *Faber v Hungary* App no. 40721/08 (ECHR, 24 July 2012), [59].
[413] Investigatory Powers Bill European Convention on Human Rights Memorandum <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473763/European_Convention_on_Human_Rights_Memorandum.pdf> accessed 6 March 2018, para 50.
[414] *K.U. v Finland* App no. 2872/02 (ECHR, 2 December 2008).
[415] ibid, [40].
[416] ibid, [50].
[417] ibid, [42-3].
[418] ibid, [46].
[419] ibid, [49].
[420] *Osman v UK* App no. 23452/94 (ECHR, 28 October 1998), [115]; *L.C.B. v UK* App no. 23413/94 (ECHR, 9 June 1998), [36].
[421] *Angelova and Iliev v Bulgaria* App no. 55523/00 (ECHR, 26 July 2007), [93].
[422] *McCann and Others v UK* App no. 18984/91 (ECHR, 27 September 1995), [161].
[423] *K.U.*, (n414), [49].

> Another relevant consideration is the need to ensure that powers to control, prevent and investigate crime are exercised in a manner which fully respects the due process and other guarantees which legitimately place restraints on crime investigation and bringing offenders to justice, including the guarantees contained in Articles 8 and 10.[424]

This demonstrates as the ECtHR in *Klass* noted 'Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.'[425] Any such measure must be necessary.[426]

It must be repeated that UK representatives before the CJEU conceded that there was no 'scientific data' to underpin the claimed need for data retention.[427] Ian Brown holds that governments have provided very little evidence that interference is proportionate and are 'prone to highlighting individual cases of repugnant crimes without any detail as to the significance of the role played by retained communications data.'[428] He makes reference to such 'sweeping claims' such as 'communications data and intercept intelligence are key factors in over 95% of the most significant investigations directed at the Serious Organised Crime groups assessed as causing the most harm to the UK.'[429] Such 'sweeping claims' were repeated in the Home Office's operational case for the retention of ICRs.[430]

The German NGO Arbeitskreis Vorratsdatenspeicherung (AK Vorrat) noted that communications data *retention* is ineffective and counterproductive for the purposes of prosecution of serious crime.[431] This is important given that the GC is willing to accept third-party statistical evidence.[432] They noted that there is no proof that the number of cleared cases, the crime rate or the number of convictions, acquittals or closed cases significantly depends on whether a blanket data retention scheme is in operation *in a given country or not*.[433] Such sentiments were echoed by Munir and Yasin who were unable to establish *how pressing the need is* 'or how often the police and security and intelligence services find it necessary to make use of such data or are significantly hampered by its absence.'[434] Section 7.1(d) demonstrated that even at an EU level, the EDPS was not convinced of the necessity of data retention, nor

---

[424] ibid, [48]; For Article 2, see *Osman*, (n420), [116].
[425] *Klass and Others v Germany* App no. 5029/71 (ECHR, 6 September 1978), [49].
[426] ibid, [59].
[427] Monika Ermert, (n68); Katie Miller, 'Why the data retention legislation should be withdrawn' (2 March 2012) <http://www.afr.com/technology/web/why-the-data-retention-legislation-should-be-withdrawn-20150227-13qufg> accessed 31 July 2017.
[428] Ian Brown, (n317), 106.
[429] ibid; Home Office, 'Protecting the Public in a Changing Communications Environment' (2009) <http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/27_04_09communicationsconsultation.pdf> accessed 29 July 2017, p10.
[430] Home Office, 'Operational Case for the Retention of Internet Connection Records' (1 March 2016) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504192/Operational_Case_for_the_Retention_of_Internet_Connection_Records_-_IP_Bill_introduction.pdf> accessed 29 July 2017, p4 and p7.
[431] Vorratsspeicherung, 'Study finds telecommunications data retention ineffective' (27 Jan 2011) <http://www.vorratsdatenspeicherung.de/content/view/426/79/lang,en/> accessed 29 July 2017; Vorratsspeicherung, 'Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics' (19 February 2011) <http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf> accessed 29 July 2017.
[432] *D.H. and Others v the Czech Republic* App no. 57325/00 (ECHR, 13 November 2007), [187]
[433] Vorratsspeicherung, Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics,' (n431).
[434] Abu Bakar Munir and Siti Hajar Mohd Yasin, (n173), 743.

were the CCC convinced when speaking in obiter dictum. The RCC criticisms were seen as criticising 'the spirit of data retention as a whole'[435] and the DCH noted the necessity and effective of data retention had not been established, even after five years.[436]

In David Anderson's *A Question of Trust*, he recommended that compulsory data to remain legal.[437] Anderson referred to statistics the European Commission used to justify the necessity of data retention,[438] but as noted above, this did not convince the EDPS of the necessity. Anderson then relied upon a 2-week detailed survey into how communications data are used.[439] Anderson does not elaborate on the *types* of communications data utilised, nor how could a two-week survey justify such wide-ranging powers. Furthermore, Anderson noted that a *quarter* of communications data requests related to threat to life, an immediate risk or urgent operational necessity in relation to serious crime or national security.'[440] These are, under EU law, the only permissible grounds for retention, highlighting that three-quarters of communications data accessed (let alone retained) is not necessary. Anderson also highlighted that 28% of requests were for communications data that were over three months old.[441] Anderson gives the example of Operation Notarise as an example of how retained data can be put to use.[442] This involved the arrest of over 600 suspected paedophiles based on 3982 requests for communications data. There are, however, problems of oversimplification, because there is no indication as to what *type* of communications data was used, how long the communications data was stored before its use, whether any data stored was a result of routine business practice or data retention laws. It is not detailed how[443] (and in what ways) the communications data was essential to identifying 92% of suspects nor whether the 336 requests for communications data older than 12 months affected the identifying suspects. It does not indicate whether other surveillance measures were used and what benefit they may have brought. Given that the suspects used TOR (a VPN), which can make communications data[444] and ICRs[445] useless, it was argued that any 'successful attack against Tor anonymity would probably have been based *on targeted surveillance* and *perhaps even on direct interference* (author's emphasis).'[446] Boiten and Hernandez-Castro noted that this strongly suggested that the National Crime Agency's (NCA) conveniently timed success 'actually lends *little evidence to support* the need for blanket data retention powers (author's emphasis).'[447] Anderson's analysis in this regard squares with the European Commission's *own* draft conclusions:

---

[435] Eleni Kosta, 'The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection' (2013) SCRIPTed 10:3 339, 349.
[436] Decision of the District Court of The Hague, Case Number C/09/480009 KG ZA 14/1575, 11 March 2015, [2.2].
[437] David Anderson, 'A Question of Trust: Report of the Investigatory Powers Review' (June 2015) <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf> accessed 30 July 2017, para 14.14.
[438] ibid, para 7.49.
[439] ibid, para 7.50.
[440] ibid, para 7.50(b).
[441] ibid, para 7.50(c).
[442] ibid, para 7.51.
[443] Eerke Boiten and Julio Hernandez-Castro, 'Can you really be identified on Tor or is that just what the cops want you to believe?'*The Conversation* (Melbourne, 25 July 2014), <https://theconversation.com/can-you-really-be-identified-on-tor-or-is-that-just-what-the-cops-want-you-to-believe-29430> accessed 30 July 2017.
[444] Leo Kelion, 'Tech firms seek to frustrate internet history log law' *BBC News* (London, 23 November 2016) <http://www.bbc.co.uk/news/technology-38068078> accessed 30 July 2017.
[445] Joint Committee on the Draft Investigatory Powers Bill, (n45), paras 133-135.
[446] Eerke Boiten and Julio Hernandez-Castro, (n443).
[447] ibid.

> [T]he *relevance* of [communications] data *decreases significantly with their age*: [70%] of *all data are use within 0-3 months of their storage* and [85%] within 0-6 months. For the added value of older data, *only anecdotal* evidence is available (author's emphasis).[448]

Brown in 2010,[449] noted that little had changed, and Anderson's observations in 2015 highlight this. This also questions the necessity of the *length* of data retention (discussed below). Some problems are also highlighted when Anderson discusses utility, where he mentions access to communications data will often be needed in *real time*[450] (therefore undermining necessity of retention). Anderson also noted that the ability to 'to extract evidence from social media and messaging'[451] (which is not the same as retaining communications data and accessing it) lead to the conviction of Imran Khawaja.[452] Thus making it unclear the role of communications data, let alone its retention in this regard.

Anderson also refers to the Director of Europol, Robert Wainwright who answers his own tautological question[453] of:

> Ask yourself what the end of data retention would mean in concrete terms? It would mean that communication data that could have solved a murder or exonerate a suspect is simply deleted and no longer available.[454]

There may be instances where communications data could solve a murder, but this question creates the impression that *without* data retention murders could not be solved. This confuses utility of communications data and its retention and sails dangerously close to a presumption of suspicion, rather than innocence. The premise of this question, simply put, is loaded. Anderson also refers to the European Commission drawing negative conclusions for law enforcement in Germany and the Czech Republic where data retention ended.[455] However, these negative consequences relied upon claims/statements (which the EDPS highlighted and wanted *evidence* of consequences *before and after* annulments).[456] Although, almost two decades ago,[457] the Earl of Northesk noted 'there is no evidence whatever that a lack of data retained has proved an impediment to the investigation of the atrocities' of 9/11.[458]

---

[448] European Commission, 'Evaluation of Directive 2006/24/EC and of National Measures to Combat Criminal Misuse and Anonymous Use of Electronic Communications (DRAFT)', Room Document <http://www.vorratsdatenspeicherung.de/images/RoomDocumentEvaluationDirective200624EC.pdf> accessed 8 August 2017.
[449] Ian Brown, (n317), 106.
[450] David Anderson, (n437), para 9.24.
[451] ibid, para 9.24(c).
[452] Sentencing remarks of Mr Justice Jeremy Baker in *R v Khawaja, Bhatti and Ali* at Woolwich Crown Court, 6 February 2015 <https://www.judiciary.gov.uk/wpcontent/uploads/2015/02/khawaja-sentencing-remarks1.pdf> accessed 31 July 2017. See [22] where it was noted that 'your interest was sufficiently profound for you to decide to travel to Syria in order to train for jihad, and it is clear from your *Facebook account* that you were showing an interest in such material for a significant period of time prior to making your decision to travel to Syria…'
[453] 'The thing to be proved is used as one of your assumptions.' A List Of Fallacious Arguments <http://www.don-lindsay-archive.org/skeptic/arguments.html> accessed 31 July 2017.
[454] David Anderson, (n437), para 9.46.
[455] ibid, para 9.47; European Commission, 'Evidence for necessity of data retention in the EU' (March 2013) <http://www.statewatch.org/news/2013/aug/eu-com-mand-ret-briefing.pdf> accessed 6 June 2017, p6 which draws upon weak correlations.
[456] Opinion of the European Data Protection Supervisor, (n55), para 50.
[457] It is accepted how technology and the way in which people use it has changed since 9/11.
[458] HL Deb 4 Dec vol 629 col. 808-9.

Anderson once again refers to Europol who compared the UK and Germany in that in the former 121 suspects were arrested or convicted and in the latter no arrests could be made.[459] But once again, such statements suffer from being vague basing the only difference in numbers on the fact the Germany did not have any compulsory data retention laws at the time. In this regard, Liberty responded to Anderson's report, noting that even with the usefulness of communications data,[460] blanket data retention was unnecessary[461] due to its *necessity* not being shown.[462]

The WP29 noted another facet of the assessment that may be important to establishing a pressing social need, public concern.[463] Chapter 5 highlighted that particularly to the UK, public concern since Snowden's revelations has largely been muted due to media bias and the government expanding powers *anyway*. Though Dimitris Potoglou *et al* has demonstrated a lack of appetite for a 12-month data retention period noting that:

> [O]n average, respondents across the EU27 were less likely to choose ISPs that retained data for more than one month and shared any type of data related to their Internet activity.

This is to some degree reflected in mass petitions across Europe and the constitutional challenges (mentioned above).[464] Anderson documents a range of threats the UK faced[465] but this does not demonstrate a pressing social need to adopt data retention measures, it just highlights the threats the UK face. It has been demonstrated that there is not a pressing social need for data retention, at the very least in the manner envisaged in the IPA 2016. The pressing social need for law enforcement purposes are weak and vague. Furthermore, Nora Ni Loideain noted all the arguments in favour of communications data retention and access were based on studies involving serious crime.[466] There was no evidence for a pressing social need for the other purposes for access to communications data (let alone its retention) for tax assessment, public health or other grounds.[467] This problem becomes more profound due to the grounds from s.61(7)(c), (d), (e), (f), (h) and (i) accounted for 0.4% requests for access to communications data in 2013[468] and 0.2% in 2015.[469] For 2015, national security accounted for 6% of requests for communications data which would make s.102(3) of the Anti-terrorism,

---

[459] David Anderson, (n437), para 14.19.
[460] Liberty, 'Liberty's briefing on 'A Question of Trust: The Report of the Investigatory Powers Review'' (June 2015) <https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%27s%20response%20to%20A%20Question%20of%20Trust%20-%20the%20report%20of%20the%20investigatory%20powers%20review_1.pdf> accessed 1 August 2017, para 14.
[461] ibid, para 37.
[462] ibid, para 45.
[463] Article 29 Working Party, (n293), para 3.14.
[464] David Anderson, (n437), para 5.66.
[465] ibid, para 3.9-3.39.
[466] Nora Ni Loideain, 'Written evidence' (2016) <https://publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB64.pdf> accessed 1 August 2017, para 1.9; Nora Ni Loideain, 'The UK Investigatory Powers Bill – one step forward, two steps back' *openDemocracy* (17 November 2015) <https://www.opendemocracy.net/digitaliberties/nora-ni-loideain/uk-investigatory-powers-bill-one-step-forward-two-steps-back> accessed 7 August 2017.
[467] ibid.
[468] 2013 Annual Report of the Interception of Communications Commissioner (HC 1184 8 April 2014), Figure 7.
[469] Report of the Interception of Communications Commissioner Annual Report for 2015, (n271), Figure 9.

Crime and Security Act 2001 (ATCSA 2001) suspect, given that national security was the *sole* ground for data retention up until it was repealed by the IPA 2016.

This subsection has demonstrated that the only ground with any supporting evidence for data retention is for fighting serious crime. This ground, however, has not sufficiently demonstrated that there is a pressing social need to allow data retention that can affect all telecommunications operators in the UK and aboard and all the communications data that can be obtained from them. For the rest of the grounds, no evidence has been provided, and so a pressing social need cannot even be countered. This lends greater weight to the reasoning of the CJEU in that data retention should only be permissible for serious crime. In any event, a pressing social has not been established because although data retention will make more communications data available, availability is not the same as necessity[470] and thus again amounts to a violation of all the relevant rights.

iii. Is there a pressing social need for a 12-month retention period?

Section 87(3) stipulates a 12-month data retention period. Such a position is likely derived from the fact that was the position in the DRR, and that AG Cruz Villalón was not convinced of the proportionality of a longer period.[471] However, AG Saugmandsgaard Øe noted that Member State courts must check whether the retention period is *based on objective criteria* such that it may be ensured that it is limited to what is strictly necessary.[472] The 12-month period is questioned by Ni Loideain in that it was noted that:

> [L]ess consideration has been given to showing detailed evidence and reasons justifying the proposed mass and indiscriminate retention period of twelve months. In other words, *an evidence-based approach is lacking* (author's emphasis).[473]

Ni Loideain took the same position with regards to ICRs,[474] therefore, an objective justification for a 12-month retention period is lacking. Yet the JCDIPB felt the case for 12-month retention periods was justified[475] mainly based on surveys[476] which either concerned *requests* for communications data or a vague statement of communications data being applicable (and therefore, not necessary). The number of requests does not, in and of itself establish necessity considering that all requests were not independently scrutinised.[477] There was a lack of detailed analysis of what communications data were necessary and for what periods of time, given that communications data is a generic term.

AG Saugmandsgaard Øe mistakenly ascribed a six-month period as acceptable based on *Zakharov*, when in fact, the GC referred to a six-month period (of intercept data) as being

---

[470] European Digital Rights 'Shadow evaluation report on the Data Retention Directive (2006/24/EC)' (17 April 2011) <https://www.edri.org/files/shadow_drd_report_110417.pdf> accessed 12 August 2017, p7.
[471] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] ECR I-845, Opinion of Cruz Villalón, [149].
[472] Opinion of Saugmandsgaard Øe, (n1), [242].
[473] Nora Ni Loideain, 'Written evidence.' (n466), para 1.5; Nora Ni Loideain, The UK Investigatory Powers Bill – one step forward, two steps back.' (n466).
[474] ibid, para 1.11.
[475] Joint Committee on the Draft Investigatory Powers Bill, (n45), para 186.
[476] ibid, para 178-9.
[477] Matthew White, (n4), 14-15.

acceptable in the *individual context*.[478] It was noted that the London Internet Exchange (LINX) recommended 'that ISPs retain log data for three to six months.'[479] At this point in time, it has not been demonstrated that there is a pressing social need for a 12-month data retention period, as this assertion is mainly based upon anecdotal evidence or assumption. This, too would lead to violations.

iv. Is there a pressing social need for Internet Connection Record, the types of (relevant communications) data, and the generation thereof?

As noted above, Articles 2 and 8 require effective criminal law and investigations. The ECtHR 'must have regard to the changing conditions within Contracting States and respond, for example, to any evolving convergence as to the standards to be achieved.'[480] Anderson recommended that the Government provide an operational case for retaining web logs.[481] The Government responded with an operational case for the retention of ICRs[482] as they comprise of web logs and much more. The operational case identifies the value of ICRs (determining who sent the messages, what service used, and ascertain access to illegal services) and some problems associated with not retaining them (difficulties in fighting online child abuse, human trafficking and fraud),[483] with examples.[484] It can be argued that allowing the retention of ICRs corresponds to the UK's positive obligations under Articles 2 and 8 given the way technology (and its use) has evolved. It could also be argued that communications data is not as serious of an interference as interception,[485] and thus the pressing social need threshold, need not be as high.

The operational case attributes the change in the way we communicate (due to technology) can exasperate the problem caused by not retaining ICRs, but admits this is not evidence in itself 'of the specific problems that law enforcement currently face.'[486] The operational case also used case studies to demonstrate damage being caused to law enforcement investigations because it is not possible to establish what communications services suspects have been using online.[487] It was noted that 862 case referrals could only be taken further it ICRs were retained.[488]

---

[478] *Roman Zakharov*, (n6), [44-48], [260]; Matthew White, The new Opinion on Data Retention: Does it protect the right to privacy?' (n86); Matthew White, (n4), 36.
[479] A review by InTechnology of legislation and regulation concerning data storage in the UK and Europe <http://www.arrowecs.co.uk/dns_cms/uploadedfiles/dns/managed_services/inpartnership/making_sense_of_data_law.pdf> accessed 7 August 2017; See also Article 29 Data Protection Working Party 'Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)]' (9 November 2004) < http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp99_en.pdf> accessed 12 August 2017, p4.
[480] *K.U.*, (n414), [44].
[481] David Anderson, (n437), para 13(b).
[482] Operational Case for the Retention of Internet Connection Records < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473769/Internet_Connection_Records_Evidence_Base.pdf> accessed 7 August 2017.
[483] ibid, p3-5.
[484] ibid, p9-11.
[485] *Liberty and Others v Government Communication Head Quarters and Others* [2014] UKIPTrib 13_77-H, 5 December 2014, [34], [111], [114].
[486] Operational Case for the Retention of Internet Connection Records, (n482), p13.
[487] ibid, p17.
[488] ibid, p14.

Chapter 3 already demonstrated why communications data retention is just as serious as interception, therefore the pressing social need for it should not be lowered. Gareth Llewellyn of Brass Horn Communications (an ISP) noted that ICRs retention will not be the panacea that the IPA 2016 envisages them to be and should therefore be removed.[489] Lyewellyn also added they will not be effective in preventing crime and are a *direct risk to the well-being of UK citizens* (author's emphasis).[490] Dr Julian Huppert argues further that operational case is 'strikingly short on detail and evidence' for the benefits from ICRs retention.[491] Huppert additionally noted that argument of the 862 referrals was 'far from clear that even with ICR retention these cases could or would be progressed; there is no evidence provided to suggest that would be the case.'[492] Huppert also noted how the failure to act on part of the police on information regarding a child abuse ring, for 14 months demonstrated that 'should focus resources on processing the data they already have' as no new powers were required.[493] Lord Paddick also noted that Mi5/6 said that ICRs are of limited value to them,[494] significantly weakening the national security case for them.

After considering the arguments for and against ICRs, the JCDIBP noted that ICRs *could prove* to be a *desirable* tool, but the Government had to address concerns of invasiveness and practicality.[495] As noted above, the ECtHR does not consider 'desirable' synonymous with 'necessary,' and as noted above, the utility of a measure in and of itself does not even ensure legality. Furthermore, the operational case did not demonstrate the pressing social need for the indiscriminate retention of ICRs,[496] which was only supported by two studies,[497] and only relates to serious crime.[498] Therefore, the pressing social need element is potentially lacking, is outweighed by the risks[499] and as ORG notes, '[t]echnology opens up possibilities for what can be done, but this does not mean it should be done.'[500] Thus, amounting to a violation.

Regarding the types of communications data that could be retained prior to the IPA 2016 i.e. in the DRR, the EDPS made a comment on the DRD (which the DRR mirrored) noting that 'it is not clear from the report whether all categories of retained data have proven to be necessary.'[501] This strikes at the heart of the justification for the data types to be retained, there has never been an operational case for anything other than ICRs and a generic reference to 'communications data' and so the necessity of each type of communications data has to be

[489] Written evidence submitted by Gareth Llewellyn on behalf of Brass Horn Communications (IPB0019).
[490] ibid.
[491] Written evidence from Dr Julian Huppert, University of Cambridge (IPB0027), para 9.
[492] ibid.
[493] ibid, p10.
[494] Alan Travis, 'Snooper's charter: GCHQ will be licensed 'to hack a major town' *The Guardian* (London, 21 June 2016) <https://www.theguardian.com/world/2016/jun/21/snoopers-charter-gchq-would-be-licensed-for-bulk-hacking> accessed 7 August 2017.
[495] Joint Committee on the Draft Investigatory Powers Bill, (n45), para 98-108.
[496] Nora Ni Loideain, 'Written evidence.' (n466), para 1.5; Nora Ni Loideain, The UK Investigatory Powers Bill – one step forward, two steps back.' (n466).
[497] ibid, para 1.7; ibid.
[498] ibid, para 1.9; ibid.
[499] *Roman Zakharov*, (n6), [302]; *S and Marper*, (n107), [99], [103]; *Digital Rights Ireland and Seitlinger and Others*, (n2), [54-5]; Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n43), Zara Rahman, para 4, p1180, Paul Bernal, para 8, p139-140.
[500] Open Rights Group, 'Internet Connection Records' <https://www.openrightsgroup.org/assets/files/pdfs/submissions/ORGSTCsubmissionIPB.pdf> accessed 7 August 2017, p9.
[501] European Data Protection Supervisor, (n55), para 63.

questioned, considering almost all communications data requests related to subscriber details (already kept by service provider irrespective of retention notices) in 2000 and just under half in 2015.[502] Without any reference to the necessity of each type of communications data, a pressing social need cannot be established, thus, resulting in a violation.

Regarding relevant communications data, as noted in Chapter 3, this encompasses a wide range of data types, including the IoTs.[503] These types of data extended beyond previous laws.[504] There has never been a pressing social need established for each and every type of communications data retained (such as email data),[505] now with the communications data types being extended, there is a greater need for justification. This is currently not the case, and thus a pressing social need has not been established, thus a violation ensues.

In relation to the retention period, it has been noted that the DRD required that those data be retained for a period of at least six months, without any distinction being made between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.[506] This demonstrates that at an EU level, the retention period should be based on communications data by type, not a general rule applicable to all. The UK previously did this in that retention periods were 12 months for subscriber information as well as telephony data, six months for SMS, EMS and MMS data, six months for e-mail data, six months for ISP data, and *four days* for web activity logs (ICRs equivalent) (author's emphasis).[507] It was explained this was chosen because 'that types of communications data, as personal data, vary with respect both to their usefulness to the agencies, and to their sensitivity.'[508] This is not to say that the retention periods under ATCSA 2001 were ECHR compatible, but it demonstrates the departure on part of the UK in distinguishing retention period by communications data type. There has been no attempt in the IPA 2016 to distinguish communications data by their sensitivity and necessity as there is a clear pressing social need to do so, ultimately resulting in a violation.

As noted above, the JCDIPB recommended that the Government clarify the types of data it expects CSPs to *generate* and in what quantities so that this information can be considered when the Bill was introduced.[509] This did not occur, and therefore, no consideration could be given to what (not defined in the IPA 2016) could be generated. Such an argument for the generation of communications data was rejected by the dCDBJC where they did not accept that Parliament should grant powers that are required only on the precautionary principle because there should *be a current and pressing need for them* (author's emphasis).[510] This ultimately means that no pressing social need has been established for the need to compel telecommunications operators to generate data, thus another violation. A similar conclusion

[502] SC Deb (F) 28 March 2000, col 252; Report of the Interception of Communications Commissioner Annual Report for 2015, (n271), Figure 6.
[503] Graham Smith, 'Never mind Internet Connection Records, what about Relevant Communications Data?' (29 November 2015) <http://www.cyberleagle.com/2015/11/never-mind-internet-connection-records.html> accessed 8 August 2017.
[504] ibid.
[505] Lexi Pimenidis and Eleni Kosta, 'The impact of the retention of traffic and location data on the internet user' (2008) DuD Datenschutz und Datensicherheit 32:2 92.
[506] *Digital Rights Ireland and Seitlinger and Others*, (n2), [63]; Opinion of Saugmandsgaard Øe, (n1), [242].
[507] Abu Bakar Munir and Siti Hajar Mohd Yasin, (n173), 739; Retention of Communications Data Under Part 11: Anti-Terrorism, Crime and Security Act 2001 <http://www.opsi.gov.uk/si/si2003/draft/5b.pdf> accessed 8 August 2017, Appendix A.
[508] ibid, Retention of Communications Data Under Part 11, para 18.
[509] Joint Committee on the Draft Investigatory Powers Bill, (n45), para 209.
[510] Joint Committee on the Draft Communications Data Bill, (n261), para 70.

can be drawn if one were to construe communications data as including 'data' in s.263(1), no pressing social need has been identified. Chapter 3 indicated how Big Data could be retained via s.263(1), s.87(9)(b) and through entity data, which pose a more serious interface with fundamental rights because data is *already* aggregated and thus the profiles (which can be biased and discriminatory) built from them are readily available. As Feiler notes, traffic analysis allows much more inferences to be made from retained data, which can include sensitive personal data.[511] This would in turn allow for fishing expeditions[512] (something Judge Pettiti warned against, see above) and continuous surveillance.[513] This potential has never been acknowledged, let alone justified. In *Tele2 and Watson* the CJEU noted that:

> [W]hile the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, *however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight* (author's emphasis).[514]

In concurrence, the UN Special Rapporteur on the right to privacy, Joseph A. Cannataci noted:

> [T]he SRP welcomes the CJEU's judgement *precisely because this evidence has not yet been made available that would persuade the SRP of the*…necessity of laws regulating surveillance which permit bulk acquisition of all kinds of data including metadata (author's emphasis).[515]

It has been demonstrated that there is no pressing social need that can justify the scope of telecommunications operators that can be covered by a retention notice, data retention in and of itself, the 12-month period of a retention notice and the types of communications data that can be retained or for what purposes.

B. Relevant and Sufficient

Another component of assessing whether a measure is 'necessary in a democratic society' is to consider whether the reasons for interference were relevant and sufficient.[516] Although the requirement is not often apparent, and its meaning obscure[517] judges Sajó and Tsotsoria regard it as:

> [A] threshold question to determine whether and how the margin of appreciation is to be applied; it is relevant in the determination of the existence of a pressing social need.[518]

---

[511] Lukas Feiler, ''The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection' (2010) 1(3) EJLT <http://ejlt.org/article/view/29/75> accessed 25 October 2017.
[512] Francesca E. Bignami, 'Privacy and Law Enforcement in the European Union: The Data Retention Directive' (2007) Chicago Journal of International Law 8 233, 235.
[513] Lukas Feiler, (n511).
[514] *Tele2 Sverige AB and Watson*, (n3), [103].
[515] Joseph A. Cannataci, 'Report of the Special Rapporteur on the right to privacy' (24 February 2017) A/HRC/34/60.
[516] *Smith and Grady v United Kingdom* App nos. 33985/96; 33986/96 (ECHR, 27 September 1999), [88].
[517] Janneke Gerards, (n385), 468.
[518] *Delfi AS v Estonia* App no. 64569/09 (ECHR, 16 June 2015), [25] of judges Sajó and Tsotsoria's dissenting opinions.

Moving from necessity to the *effectiveness* of a measure is something that the ECtHR already entertains.[519] Though Janneke Gerards holds that the real challenge lies in applying the test in more difficult cases, where *it needs to rely on factual, statistical, or empirical information as to the effectiveness of a certain measure* (author's emphasis).[520] If the margin of appreciation is narrowed, then the demands of the effectiveness need to be higher in which the state has to demonstrate, justify with evidence and the ECtHR to assess.[521]

In *S and Marper*, the GC looked to statistics consider whether the UK's justification for DNA/finger print retention was relevant and sufficient.[522] The GC concluded that *despite* neither statistics or examples provided by the UK in themselves establish that the successful identification and prosecution of offenders could not have been achieved without the permanent and indiscriminate retention it accepted that extension of the database had nonetheless contributed to the detection and prevention of crime.[523] This Chapter is not here to discuss this problematic formulation by the GC in *S and Marper*[524] but to highlight a distinction in which the ECHR requires a stricter interpretation regarding the effectiveness. The interferences of communications data retention extend beyond what was envisaged in *S and Marper* in that it mainly affects persons who will *never* be connected to or suspected of a crime, it retains *much more* intrusive data, and it does not just interfere with Article 8. In this regard, the margin of appreciation should be narrower than in *S and Marper*, and the justifications more compelling.

Given that an operational case was only given for ICRs, the focus of effectiveness will focus upon them first. Tim Panton, a software developer considered the 3 operation values (mentioned above) of ICRs and gave it a '4/10' in achieving its operational objectives.[525] Panton, did however, note that falling into the wrong hands, much more could be learnt which would be useful for identity thieves and robbers.[526] Others have highlighted that the operational value of ICRs is based on the assumption that online criminals will not employ methods to avoid detection such as VPNs, proxy web browsers etc.[527] The retention would push internet traffic (legitimate and otherwise) into more protected spaces (such as Tor's mobile ORBOT which anonymises internet traffic)[528] leaving almost exclusively a database[529] of innocent

[519] Janneke Gerards, (n385), 473.
[520] ibid.
[521] ibid, 476, 478, and 481.
[522] *S and Marper*, (n107), [114].
[523] ibid, [117].
[524] The GC accepted that the evidence presented by the UK did not actually aid the prevention and detection of crime, but accepted that it did so nonetheless. This uncritical approach is contradictory to the effective protection of Convention rights, especially when the GC accepted that the margin was narrower; ibid, [112].
[525] Tim Patron, 'The Investigation of Packets' (13 November 2015) <https://babyis60.wordpress.com/2015/11/13/the-investigation-of-packets/> accessed 9 August 2017; Written evidence submitted by Tim Panton (IPB0016).
[526] ibid.
[527] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n43), Liberty, para 47, p868, IT-Political Association of Denmark, para 27, p705-6; George Danezis, 'Traffic Data Retention Impact on civil society organizations' <https://pdfs.semanticscholar.org/8c8f/606fd68f661457011d611b6cf9ac8050f297.pdf> accessed 10 August 2017.
[528] Tor, 'Tor on Android' <https://www.torproject.org/docs/android.html.en> accessed 10 March 2018.
[529] Demonstrates how long an ICR would be for one online action - RevK's Rants 'What is an "Internet Connection Record"?' (14 November 2016) <http://www.revk.uk/2015/11/what-is-internet-connection-record.html> accessed 9 August 2017.

citizens lives, an *ineffective strategy*,[530] which can contribute to the *escalation* of crimes (author's emphasis).[531] Identifying suspects is limited as it only identifies the device used as the data is 'inexact and error-prone.'[532] ICRs would also not aid in missing children cases because of the 'always on' connection therefore not indicating *when* a service was used[533] nor would it be practical for an ISP to indicate that the missing person accessed Twitter (if at all) before vanishing (author's emphasis).[534] Not only was the idea of retaining ICRs questionable,[535] data retention in itself was argued to not be viable in the long term.[536] Some have argued ICRs will generate misleading results, Adrian Kennard demonstrated that visiting his blog would create an ICR for pornhub.com.[537] Daniel Walrond highlighted that this is very important such ICRs could be generated for 'hate websites, child pornography, how to make a bomb, and how to circumvent being tracked by'[538] the IPA 2016.

It has also been noted that illegal websites create a needle in the haystack problem as Denmark experienced.[539]In their written submission to the JCDIPB, the IT-Political Association of Denmark discussed the Danish equivalent of ICRs retention which was dropped for lack of effectiveness.[540] The Ministry of Justice published a self-evaluation report about Danish data retention noting that it had only been used in a limited number of cases, even within the intelligence community.[541] Due to ineffectiveness of achieving said aim, the Ministry of Justice decided to repeal session logging.[542] The JCDIPB accepted that the highlighted differences between the UK and Danish system, and that the UK had learnt lessons from the Danish failure in using session logging data for investigating and prosecuting criminal offences.[543] The JCDIPB recommended that the Government publish a full assessment of the differences between Danish session logging and ICRs retention.[544] However, as the IT-Political Association of Denmark later noted 'the Home Office comparison is much less clear in describing what the UK ICR implementation *will do differently and why it will work*' (author's emphasis).[545] For this reason, its lack of effectiveness, its expensiveness, intrusiveness and lack of proportionality, it was recommended that ICRs retention be dropped.[546] Some form of data

[530] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n43), Liberty, para 47, p868; George Danezis, 'Covert Communications Despite Traffic Data Retention' <http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/cover.pdf> accessed 10 August 2017.
[531] Peter Shields, 'Electronic Networks, Enhanced State Surveillance and the Ironies of Control' (2006) Journal of Creative Communications 1:1.
[532] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n43), Liberty, para 48, p868.
[533] ibid, Andrews & Arnold Ltd, p62.
[534] ibid.
[535] ibid, p63.
[536] ibid, p64.
[537] Joint Committee on the Draft Investigatory Powers Bill, *oral evidence*, (n256).
[538] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n43), Daniel Walrond, p1345.
[539] ibid, IT-Political Association of Denmark, para 26, p705.
[540] ibid, para 2, p701.
[541] ibid, para 9, p702; 'Redegørelse om diverse spørgsmål vedrørende logningsreglerne' (December 2012) <http://www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf> accessed 10 August 2017; There is no English translation but it is covered in Torben Olander, 'In Denmark, Online Tracking of Citizens is an Unwieldy Failure' (22 May 2013) <http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy> accessed 10 August 2017.
[542] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n43), para 12, p 702; Press Release: The Minister of Justice repeals the rules for session logging (2 June 2014) <http://justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2014/justitsministeren-oph%C3%A6ver-reglerne-om-sessionslogning> accessed 10 August 2017.
[543] Joint Committee on the Draft Investigatory Powers Bill, (n45), para 146.
[544] ibid, para 147.
[545] Written evidence: IT-Political Association of Denmark (IPB20), para 5.
[546] ibid, paras 31-35.

retention in Denmark, has however, re-emerged.[547] It is inconceivable based on the arguments against ICRs retention for there to be a sufficient reason to justify this power and in the manner it can be exercised.

Continuing with data retention in other European countries. A comprehensive analysis of data in the Netherlands highlighted that although the value of traffic data is clear from court rulings, they shed no light on the *age* of the requested data (author's emphasis).[548] The District Court of the Hague (DCH) noted that the necessity of data retention had not been established.[549] It has already been noted above by the EDPS, WP29, Commission and AK Vorrat the assumed effectiveness of data retention is utterly questionable.[550] Moreover, the needle in the haystack problem creates the 'false positive' and 'false negative' problem.[551]

It was already argued that a pressing social need for data retention could not be sustained because most of the evidence was either anecdotal, conflated the utility of communications data with its retention. Furthermore, arguments in favour of communications data retention did not detail what actual communications data were necessary in anecdotal cases, why all communications data needed to be retained for 12-months, nor an operational case for all the types of communications data that could be retained or generated. Finally, and probably most importantly it was never explained why the obligation to retain expanded to essentially anything that could communicate, making one's home a personal Panopticon. Some of the reasons are not only insufficient, but non-existent.

As the ECtHR in *Sunday Times v United Kingdom*[552] noted, it is not sufficient that the interference involved belongs to that *class of the exceptions* i.e. national security, nor is it sufficient that the interference was imposed *because its subject-matter fell within a particular category or was caught by a legal rule formulated in general or absolute terms* (author's emphasis). The ECtHR has to be satisfied that the interference was necessary having regard to the facts and circumstances prevailing in the specific case before it.[553] However, even if it is to be argued that the arguments in favour of the scope of data retention obligations are deemed to be relevant, this does not equate to them being sufficient.[554] It has been strongly demonstrated that the reasons elucidated to are not sufficient, and thus would lead to a violation.[555]

C. Proportionality

[547] IT-Pol, 'Denmark allows massive retention of location data for mobile internet' (28 June 2017) <https://edri.org/denmark-allows-massive-retention-of-location-data-for-mobile-internet/> accessed 11 August 2017.
[548] G. Odinot, D. de Jong, R.J. Bokhorst and C.J. de Poot, 'The Dutch implementation of the Data Retention Directive' (2014) <https://www.wodc.nl/binaries/ob310a-full-text_tcm28-78190.pdf> accessed 9 August 2017, p133.
[549] Decision of the District Court of The Hague, (n436), [2.2].
[550] Mariuca Morariu, 'How Secure is to Remain Private? On the Controversies of the European Data Retention Directive' Amsterdam Social Science 1:2 46, 61; Theodore Konstadinides, 'Mass Surveillance and Data Protection in EU Law: The Data Retention Directive Saga' in Maria Bergström and Anna Jonsson Cornell (ed) *European Police and Criminal Law Co-Operation* (Swedish Studies in European Law (5), Hart Publishing, Oxford, 2014).
[551] Lukas Feiler, (n511). In this context, a 'false positive' signifies an individual who is incorrectly identified as a 'terrorist.' A 'false negative' signifies a terrorist incorrectly identified as 'not a terrorist.'
[552] *Sunday Times v United Kingdom*, (n114), [65].
[553] ibid.
[554] ibid, [63].
[555] ibid, [67].

Proportionality appears prevalent in many forms[556] though in the context of the ECtHR it has often been described as 'striking a fair balance'[557] between the interests (or right of the individual)[558] at stake.[559] In this assessment of proportionality, which is 'inherent in the whole of the Convention'[560] it is important to consider numerous factors,[561] such as whether retention strikes at the substance of the right, whether there was a least restrictive measure to achieve said objective, and whether the fair balance has been struck given all the circumstances.

a. Striking at the substance of the Right?

Chapter 3 highlighted how communications data retention interferes with the very substance/essence of the right to Article 8 in terms of the seriousness of the interference. Chapter 4 highlighted how data retention strikes at the freedom of communication in relation to Article 10, which forms the basis of the substance of Article 10. Chapter 4 further noted forced disclosure and making the possibility of deducing religious beliefs would interfere with Article 9. Further, the ECtHR has noted that to construe Article 9 as permitting every kind of compulsion with a view to the disclosure of religion or belief would strike at the very substance of the freedom it is designed to guarantee.[562] As Taylor notes if a measure impairs the very essence of the right it will almost certainly be disproportionate.[563] Although Article 11 and Article 2 Protocol 4 were not discussed specifically, it is maintained that a measure unjustified under Article 8(2) *ipso facto constitutes an unjustified interference with* those said rights.

b. Least Restrictive Measure

Brems and Lavrysen describe the concept of a least restrictive measure (LRM) as using a nutcracker, instead of a sledgehammer to crack a nut.[564] In *Nada v Switzerland* it was noted that for a measure to be proportionate and necessary, the possibility of recourse to a less damaging measure to fundamental rights which fulfils the same aim *must* be ruled out.[565] *Glor v Swtizerland*[566] is the first ECtHR case that states the LRM rule as a general principle, regardless of the Convention provision invoked and regardless of the context of the case.[567] In *Schweizerische Radio- und Fernsehgesellschaft SRG v Switzerland*[568] the ECtHR took a procedural[569] and substantive[570] view of the LRM principle.

---

[556] Thomas Hickman, 'Proportionality: Comparative Law Lessons' (2007) 12 Jud. Rev. 31.
[557] *Hatton v UK* App no. 36022/97 (ECHR, 8 July 2003), [123].
[558] *Reiner v Bulgaria* App no. 46343/99 (ECHR, 23 May 2006), [141].
[559] *Sahin v Germany* App no. 30943/96 (ECHR, 8 July 2003), [48].
[560] *N v UK* App no. 26565/05 (ECHR, 27 May 2008), [44].
[561] Nick Taylor, 'Policing, privacy and proportionality' (2003) E.H.R.L.R. Supp (Special issue: privacy 2003), 86, 88.
[562] *Sinan Isik v Turkey* App no. 21924/05 (ECHR, 2 February 2010), [42].
[563] Nick Taylor, (n561), 88.
[564] Eva Brems and Laurens Lavrysen, ''Don't Use a Sledgehammer to Crack a Nut': Less Restrictive Means in the Case Law of the European Court of Human Rights' (2015) HRLR 15:1 139, 140.
[565] *Nada v Switzerland* App no. 10593/08 (ECHR, 12 September 2012), [183].
[566] *Glor v Switzerland* App no. 13444/04 (ECHR, 30 April 2009), [94].
[567] Eva Brems and Laurens Lavrysen, (n564), 155.
[568] *Schweizerische Radio- und Fernsehgesellschaft SRG v Switzerland* App no. 34124/06 (ECHR, 21 June 2012), [61].
[569] Eva Brems and Laurens Lavrysen, (n576), 150. 'In a procedural test, a court examines whether the decision-making body has duly considered whether there is an LRM available or not.'
[570] ibid, 'In a substantive test, on the other hand, the court has to make its own assessment of the possibility and effectiveness of an LRM, regardless of the decision-making body's own assessment.'

Although Brem and Lavrysen acknowledge that there is no clear affirmation of the LRM in general terms,[571] ECtHR case law is clearer in the surveillance context. In *Zakharov* the GC affirmed its case law in determining whether it is possible to achieve the aims by less restrictive means.[572] An example of a LRM is individual measures are less restrictive than measures affecting a plurality of individuals.[573] Thus in *Klass*, the ECtHR accepted that German law confined secret surveillance to where there were factual indications of suspicion of serious crimes, where other measures were without the prospect of success or considerably more difficult, thus preventing *general surveillance*.[574]

One suitable alternative to data retention, argued by many[575] is what is known as 'data preservation.'[576] Data preservation also known as *quick freeze* and *freeze plus* in which communications data is temporarily secured relating only to specific suspects of criminal activity, which may subsequently be made available to law enforcement authorities through judicial authorisation (author's emphasis).[577] Data preservation is argued to be a LRM in relation to data retention because it will likely only affect 1% of the population,[578] is less intrusive to privacy[579] and other fundamental rights in terms of the scale and number of people it affects.

Although not mentioned as a principle within cases concerning LRM, judge Pinto de Albuquerque regarded a LRM should be equally effective to the measure in question.[580] It has been argued by the UK that data preservation is futile,[581] and 'wholly impracticable.'[582] The JCDIPB accepted that preservation was not a viable alternative as they do not provide retrospective information and would be of limited value in instances where criminal action had ceased.[583] In any event, the ECtHR would need to consider the reasonableness of the national authorities' choice between a slightly more effective measure that is more detrimental to individual interests and a rather less effective, but also less restrictive provision.[584] Though, arguments about not being sure who might become suspects and therefore not being sure about which data to retain for the future really does sound like the pleadings of a paranoid police

[571] Eva Brems and Laurens Lavrysen, (n576), 156.
[572] *Roman Zakharov*, (n6), [260].
[573] Eva Brems and Laurens Lavrysen, (n576), 143; Eva Brems, 'Human Rights: Minimum and Maximum Perspectives' (2009) HRLR 9:3 349, 360.
[574] *Klass*, (n425), [51].
[575] Ian Brown, (n317), 107-8; Abu Bakar Munir and Siti Hajar Mohd Yasin, (n173), 741, 747-9, 751; Article 29 Data Protection Working Party, (n479), p4; Open Rights Group, 'Digital Surveillance' <https://www.openrightsgroup.org/assets/files/pdfs/reports/digital-surveillance.pdf> accessed 12 August 2017, p47-50; Foundation for Information and Policy 'FIPR response to the retention of communications data consultation' <http://www.fipr.org/030530retention.html> accessed 12 August 2017; Opinion of the European Data Protection Supervisor, (n55), para 51-55; European Digital Rights, (n470), p6-7; All Party Parliamentary Internet Group, 'Communications Data: Report of an Inquiry by the All Party Internet Group' (January 2003) <https://www.cl.cam.ac.uk/~rnc1/APIG-report-commsdata.pdf> accessed 12 August 2017, para 189-190.
[576] Clive Walker and Yaman Akdeniz, 'Anti-Terrorism Laws and Data Retention: War is Over?' (2003) NILQ 52:2 159, 177; The Czech Republic Constitutional Court, (n51), [55].
[577] European Data Protection Supervisor, (n55), para 54.
[578] Open Rights Group, (n575), p47.
[579] European Data Protection Supervisor, (n55), para 56.
[580] *Mouvement Raëlien Suisse v Switzerland* App no. 16354/06 (ECHR, 13 July 2012).
[581] Clive Walker and Yaman Akdeniz, (576), 177.
[582] *Davis & Ors*, (n163), [70].
[583] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n43), para 183.
[584] Janneke Gerards, (n385), 484.

state.[585] Also, the retrospective aspect of data retention, assumes that in the absence of data retention, no data is available, as this was not the case in the aftermath of the Madrid bombings,[586] and in the UK, both in the aftermath of 9/11[587] and the London bombings, ISPs voluntarily preserved data.[588] In relation to the 9/11 preservations, Detective Inspector Mike Ford of the National Hi-Tech Crime Unit said 'I can assure you that the existence of the data has been of significant benefit and value.'[589]

Given that it has been argued data retention is not necessary, even if data retention was more effective than preservation the fact that the LRM scores worse on cost–benefit analysis is irrelevant.[590] Moreover, any added effectiveness of data retention is minimal and the associated financial and privacy costs are high.[591] The likelihood of being able to identify threats out of vast stores of data absent an initial lead is practically zero, even if content were monitored.[592] Evidence presented to the Commission concluded that 'data retention and data preservation are complementary rather than alternative instruments.'[593] However, the study noted that three Member States (did not state which) stated that data preservation is never or rarely used, and seven noted that no statistics were available,[594] therefore, drawing questions on comparability of conclusions. Only 14 countries took part in the *survey*, that displayed no statistical evidence, and thus suffers from similar criticisms the EDPS highlighted with the Commission's report. Furthermore, as European Digital Rights (EDRi) pointed out, Austria, Germany, Greece, Norway, Romania, Sweden and Canada all use data preservation instead of retention. They continued that the absence of data retention legislation did not lead to a rise in crime in those states, or to a decrease in crime clearance rates, not even in regard to Internet crime. Nor did the coming into force of data retention legislation have any statistically significant effect on crime or crime clearance.[595]

Data preservation is a position preferred by the CoE as noted in Article 16 of the Budapest Convention,[596] and despite criticisms,[597] the UK ratified in 2011. Although the ECtHR has frequently based its finding of a violation (amongst others) on the national authorities' lack of consideration of less restrictive alternatives,[598] in *Soltsyak v Russia*[599] the ECtHR demonstrated that a violation can occur without considering the fair balance to be struck between rights and

[585] Clive Walker and Yaman Akdeniz, (576), 177.
[586] European Digital Rights, (n470), p13.
[587] All Party Parliamentary Internet Group, (n574), para 182.
[588] Ian Brown, (n317), 108.
[589] All Party Parliamentary Internet Group, (n575), para 182.
[590] Eva Brems and Laurens Lavrysen, (n576), 144.
[591] Ryan Hansen, 'Data Preservation: An Effective Approach to Combating Internet Crime in the UK' (2003) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=947371> accessed 12 August 2017.
[592] ibid.
[593] Centre for Strategy and Evaluation Services, 'Evidence of Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries' (2012) <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/police-cooperation/data-retention/docs/drd_task_2_report_final_en.pdf> accessed 13 August 2017, p23.
[594] ibid, p17.
[595] European Digital Rights, (n470), p15.
[596] Council of Europe's Convention on Cybercrime ETS No. 185, 23.XI.2001; Ian Brown, (n317), 107; European Digital Rights, (n470), p6; All Party Parliamentary Internet Group, (n575), para 108.
[597] Clive Walker and Yaman Akdeniz, (576), J Fisher, 'The Draft Convention on Cybercrime: Potential Constitutional Conflicts' (2001) 32 U.West.L.A. L.Rev. 339; Article 29 Working Party, 'Opinion 4/2001 On the Council of Europe's Draft Convention on Cyber-crime' <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp41_en.pdf> accessed 13 August 2017.
[598] Eva Brems and Laurens Lavrysen, (n576), p157.
[599] *Soltysyak v Russia* App no. 4663/05 (ECHR, 10 February 2011), [53-55].

competing interests.[600] This case concerned banning the movement of an ex Russian serviceman on the grounds preventing the transmission of confidential information. In this case, the ECtHR noted the ineffectiveness of this measure as confidential information could be passed on without leaving the country.[601] This Chapter noted the ease at which blanket data retention can be circumvented for e.g. by use of a VPN. Therefore, due to the narrowed margin of appreciation,[602] it is argued that a violation should be found for a LRM (data preservation) being effectively ruled out with compelling evidence.

c. Fair Balance?

The fair balance principle of the ECtHR's case law was established very early in its history.[603] As Alastair Mowbray noted, Articles '8-11…by their qualified structures have provided further justification for the Court applying the principle.'[604] This is also the case for Article 2 Protocol 4.[605] The function of the fair balance principle is to assess the proportionality of the State's conduct.[606] The ECtHR 'has also taken account of other factors when utilising the fair balance principle.'[607] It is these various factors that will form the basis of the consideration of the fair balance principle.

i. Blanket and indiscriminate data retention is disproportionate

In *S and Marper*, not only was the GC struck[608] blanket indiscriminate nature of data retention, they ruled that it:

> *[Failed] to strike a fair balance between* the competing public and private interests and that the respondent State has *overstepped any acceptable margin of appreciation* in this regard. Accordingly, the retention at issue *constitutes a disproportionate* interference with the applicants' right to respect for private life and *cannot be regarded as necessary in a democratic society* (author's emphasis).[609]

In the specific context of communications data retention, as noted above, the CJEU ruled that EU law precludes the 'general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.'[610] For the HC, it was difficult to conceive how the tests of necessity and proportionality could require the retention of all communications data due to the wording of 'all data' in the IPA 2016.[611]

However, as Lord Kerr noted, it is the *potential reach of the power* that needs to be assessed. Moreover, the GC goes further than the CJEU in this regard because it was found that data retention even within the confines of specific (suspects but not convicts) parameters was

[600] Janneke Gerards, (n385), 471.
[601] *Soltysyak v Russia*, (n599), [52-53].
[602] Janneke Gerards, (n385), 480-481, 487; Eva Brems and Laurens Lavrysen, (n576), 151.
[603] Alastair Mowbray, 'A Study of the Principle of Fair Balance in the Jurisprudence of the European Court of Human Rights' (2010) Human Rights Law Review 10:2 289, 290.
[604] ibid, 316, 303-307.
[605] *De Tommaso v Italy* App no. 43395/09 (ECHR, 23 February 2017), [104].
[606] Alastair Mowbray, (n603), 308.
[607] ibid, 312.
[608] *S and Marper*, (n107), [119].
[609] ibid, [125].
[610] *Tele2 Sverige AB and Watson*, (n3), [134(1)].
[611] *Liberty*, (n99), [129].

disproportionate. If a retention notice is imposed upon only one or a select number of telecommunications operators, this could satisfy EU law because it could be argued that this is not a catch all power. Such a position doubtful,[612] moreover, if one considers *S an Marper*, a retention notice on *one* telecommunications operator would still constitute a disproportionate interference with fundamental rights. An example is British Telecoms (BT), who has over nine million broadband subscribers.[613] If a retention notice is served upon BT, nine million subscribers can have their rights interfered with, a discriminatory indiscriminate power.[614] This leads to the next issue, most people whose communications data are retained bear no relation to the purposes of retention.

ii. Most retained data are of innocent people

As many have noted above, most retained data is of innocent people, who bear no relation (or ever will) to the aims to which retention notices can be issued. In *Zakharov*, the GC noted that the automatic storage for six months of clearly irrelevant data cannot be justified under Article 8.[615] It would be for the State to justify why such the amounts of data retainable is relevant, which is not possible. This, of course would also be true for the other Convention Rights engaged based on the *ipso facto* idea of violations elucidated to above. Given that most communications data retained is irrelevant, this highlights the importance of data retention not being an individual issue, but a societal one.

iii. Does not even comply with Tele2 and Watson

Jennifer Cobbe has argued that the IPA 2016 does not satisfy the requirements of *Tele2 and Watson* because, amongst other things:

a. Retention notices can be issued in pursuit of a range of purposes other than those permitted.
b. Retention is indiscriminate and is the rule rather than the exception.
c. The length of the retention period is not objectively determined and limited to what is strictly necessary.
d. IPA does not provide clear and precise rules governing the scope and application of retention.[616]

The ECtHR in *Big Brother Watch* noted that (although in relation to whether a measure was in accordance with the law) where UK and EU law diverge, EU law takes primacy, and if UK law does not conform with EU law, there will be a violation of Article 8.[617]

iv. The Social Value of Privacy and its underpinning of other Fundamental Rights and Democracy itself

[612] Matthew White, (n27); Jennifer Cobbe, (n93), 18; Andrew D. Murray, (n165), 161.
[613] Mark Jackson, 'UK ISP BT Tops 9 Million Broadband Users, 4.1M on Superfast Fibre FTTC' (5 May 2016) <http://www.ispreview.co.uk/index.php/2016/05/uk-isp-bt-top-9-million-broadband-users-4-1m-fibre-broadband.html> accessed 15 August 2017.
[614] Matthew White, (n4), 38.
[615] *Roman Zakharov*, (n6), [255].
[616] Jennifer Cobbe, (n93); Jennifer Cobbe, 'Casting the Dragnet: Communications Data Retention under the Investigatory Powers Act' (2017) <https://www.academia.edu/33709047/Casting_the_Dragnet_Communications_Data_Retention_under_the_Investigatory_Powers_Act> accessed 20 September 2017.
[617] *Big Brother Watch*, (n323), [466-468].

When balancing rights and competing interests, 'States have quite often relied upon rather general assertions of community interests'[618] against individual rights, making it seem 'extravagant when weighed against the interests of society as a whole.'[619] In the context of data retention, such an individualised position is no longer sustainable as it can affect all the population, significant portions of it, or simply put, more than one person at any given time. Moreover, framing the debate as privacy v security misconstrues the debate because 'as both can be portrayed as social interests.'[620] It is this social interest/value/benefit of privacy that is important when considering[621] the fair balance regarding data retention as the necessity and proportionality have to be clearly 'demonstrated *by considering that privacy is not only an individual right* of control over one's information, *but moreover a key element of a democratic constitutional order* (author's emphasis).'[622] Moreover, '[i]t is hard to imagine, for example, being able to enjoy freedom of expression, freedom of association, or freedom of religion without an accompanying right to privacy.'[623] The GFCC also noted that 'the storage of telecommunications traffic data without cause is capable of creating a diffusely threatening feeling of being watched which can impair a *free exercise of fundamental rights in many areas*' (author's emphasis).[624]

Not only is privacy important for other fundamental rights as noted in Chapter 4, it has a social value. Hughes noted that ECtHR has not developed a strong notion of the role of privacy as a bulwark against totalitarianism.[625] As Tumay notes:

> The *only goal* of these restrictions must be the *restoration of the normal functioning of the society*. The *restrictions must not overste*p, in the scope of their subject-matter, the *borders determined by this goal* (author's emphasis).[626]

The ECtHR in *Szabo and Vissy* highlighted the social value of privacy when recognised that '[i]n a field where abuse is potentially so easy in individual cases and *could have such harmful consequences for democratic society as a whole* (author's emphasis).' [627] In *Zakharov* the GC believed that '*the values of a democratic society* must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded (author's emphasis).'[628]

---

[618] Alastair Mowbray, (n603), 312.
[619] Daniel Solove, *Understanding Privacy* (Harvard University Press 2009), 89.
[620] Arthur J. Cockfield, 'Protecting the Social Value of Privacy in the context of State Investigations using New Technologies' (2007) U.B.C. Law Review 40:1 41, 41-42.
[621] Daniel J. Solove, (n619), 89.
[622] Lilian Mitrou, 'Communications data retention: a Pandora's box for rights and liberties' in Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis and Sabrina di Vimercati (eds) *Digital privacy: Theory, technologies, and practices* (Auerbach Publications 2007), 425.
[623] Benjamin J. Goold, 'Surveillance and the Political Value of Privacy' (2009) Amsterdam Law Forum 1:4 3, 4.
[624] BVerfG, (n176), [212].
[625] Kirsty Hughes, 'The social value of privacy, the value of privacy to society and human rights discourse' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy Interdisciplinary Perspectives* (Cambridge University Press), 234.
[626] Murat Tumay, 'The Concept Of 'Necessary In A Democratic Society' In Restricton Of Fundamental Rights A Reflection From European Convention On Human Rights' (2011) Human Rights Review I:2, 2.
[627] *Szabo and Vissy*, (n152), [77].
[628] *Roman Zakharov*, (n6), [233].

Taking into account the social value of privacy has been implicitly recognised by the Supreme Court of Canada (SCC).[629] *R. v. Duarte*[630] concerned the investigation into alleged drug trafficking, the police rented an apartment for a police informer and equipped the apartment with audio-visual recording equipment installed in a wall.[631] The SSC stated that:

> A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made…might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning.[632]

The SCC continued that 'the relevant question is not whether criminals must bear the risk of warrantless surveillance, but whether it should be *imposed on all members of society* (author's emphasis)'[633] as privacy 'is the very hallmark of a free society.'[634] For Cockfield, these views serve as to acknowledge the 'importance of the social value of privacy'[635] something which the ECtHR can[636] and should take account of. This relates to data retention in that as noted above, retention is not based on reasonable suspicion of individual conduct, but service used. Boehm and de Hert highlighted:

> Measures such as data retention or 'fishing expeditions' by the police or the secret service *increasingly target a greater number of individuals than the 'traditional' surveillance techniques* (author's emphasis).[637]

When data retention is looked at through the lens of what privacy i.e. Article 8, underpins (a collection of other Convention Rights and democracy itself) and the collective social value it brings, any kind of measure that interferes with these rights in a blanket and indiscriminate manner cannot said to be striking a fair balance with those said rights, on an individual level, and more importantly *on a societal one*. This, as said above, would be the case if a retention notice was served on every telecommunications operator, or just one as with the social value of privacy, any unjustified interference creates a social harm.

v. Social Harms

Although referring to the severity of interference, Feiler noted, 'the social harm potentially created' should be considered when determining the proportionality of data retention.[638]

a. Chilling Effect

[629] Arthur J. Cockfield, (n620), p53.
[630] *R. v. Duarte*, [1990] 1 S.C.R. 30.
[631] Arthur J. Cockfield, (n620), p53.
[632] *R. v. Duarte*, (n630), [44].
[633] ibid; *Commonwealth v. Thorpe*, 424 N.E.2d 250 (1981), [258].
[634] *R. v. Duarte*, (n630), [53].
[635] Arthur J. Cockfield, (n620), p54.
[636] *Hirst v UK* App no. 74025/01 (ECHR, 6 October 2005), [35-37]; Kanstantsin Dzehtsiarou, 'Comparative Law in the Reasoning of the European Court of Human Rights' (2010) University College Dublin Law Review 10 109; Eirik Bjorge, 'National supreme courts and the development of ECHR rights' (2011) Int J Const Law 9:1 5.
[637] Franziska Boehm and Paul de Hert, *The rights of notification after surveillance is over: ready for recognition?* (Yearbook of the Digital Enlightenment Forum 2012, IOS Press).
[638] Lukas Feiler, (n511).

The chilling effect has already been mentioned in this Chapter and others but it is the 'the fear of being watched or eavesdropped upon makes people change their behaviour, even behaviour that is not illegal or immoral.'[639] Feiler asked what extent will data retention have a chilling effect on the exercise of people's fundamental rights? He continued that if behavioural modifications do ensue, what are the sociological effects? He asked would social minorities (based on political views, income class, religion, or any other factor) feel pressured to assimilate to the mainstream so as not raise any suspicions? Probably the most poignant question: Haven't most positive sociological developments been started by a social minority - that might now be deterred from deviating from what is considered appropriate by the majority?[640]

David Anderson questioned the chilling effect to which the CJEU ascribed to, noting:

> [A] more rigorous analysis of proportionality would have focused on any actual harm that this useful power might be shown to have caused over its years of operation, and sought to avoid assertions based on theory or on informal predictions of popular feeling.[641]

It is important, and ironic to note that, data retention legislation, especially the DRD *were* 'based on theory or on informal predictions' of its utility. As Lord Kerr in his dissenting judgment in *Beghal v DPP* noted, 'powers which can be used in an arbitrary or discriminatory way are not transformed to a condition of legality simply because they are of proven utility.'[642] Moreover, Anderson's argument would seemingly fall into the narrow nothing-to-hide-like argument that looks for singular type of injury, be it some grave physical violence, a loss of substantial money or something severely embarrassing.[643] To consider privacy harms in that way would result in fewer privacy problems being recognised.[644] This of course would make fundamental rights protections theoretically and illusory if individuals would have to prove *actual* harm, data retention in and of itself *is* the initial harm, especially when it affects the vast majority of people who are in no way connected to criminal activity. When Australia enacted data retention laws, Virtual Private Network (VPN) NordVPN reported a 100% increase in users which they noted that '[i]t's common for people to turn to VPNs when anti-privacy laws are passed.'[645] An increase in UK usage was also reported in the UK when the IPA 2016 and Digital Economy Act 2017 were being passed.[646] Or by the increasing the use of ad blockers

---

[639] Rozemarijn van der Hilst, 'Human Rights Risks of Selected Detection Technologies: Sample Uses by Governments of Selected Detection Technologies' (2009) <http://www.detecter.bham.ac.uk/D17.1HumanRightsDetectionTechnologies.doc> accessed 11 March 2018, p20.

[640] Lukas Feiler, (n511).

[641] Bingham Centre for the Rule of Law, 'Meeting Report: EU Law, the Investigatory Powers Act, and UK-EU Cross-Border Crime and Security Cooperation' (17 March 2017) <https://www.biicl.org/documents/1634_2017-04-29_-_appg_report_14_march_2017.pdf?showdocument=1> accessed 22 June 2017, p8.

[642] *Beghal*, (n168), [93].

[643] Daniel Solove, *Nothing to Hide. The False Trade-off between Privacy and Security* (Yale University Press 2011), 29.

[644] ibid.

[645] Asha McLean, 'Data-retention legislation sending Australians into the arms of VPN providers' *ZDNet* (2 June 2017) <http://www.zdnet.com/article/data-retention-legislation-sending-australians-into-the-arms-of-vpn-providers/> accessed 24 June 2017.

[646] Jon Martindale, 'UK VPN usage explodes as Digital Economy Bill progresses' (20 December 2016) <https://www.kitguru.net/gaming/security-software/jon-martindale/uk-vpn-usage-explodes-as-digital-economy-bill-progresses/> accessed 11 September 2017.

in which 11 million devices in the UK now have.[647] As Edward Snowden revealed 'government surveillance efforts are sometimes bolstered by online advertising practices'[648] making it more difficult to ensure privacy, security and anonymity.

Rozemarijn van der Hilst noted that according to a German poll on the effects of the implementation of the DRD, 52% said they would not use telecommunications to contact drug counsellors, psychotherapists or marriage counsellors and 11% said they had already abstained from using phone, cell phone or email in certain occasions.[649] Mitrou also found that '[u]nder pervasive surveillance, individuals are inclined to make choices that conform to mainstream expectations.'[650] Valerie Aston by implication, highlighted that data retention has the potential to result in an intrusion into psychological integrity, as well as limiting personal autonomy.[651]

As David Kaye noted, surveillance can create a chilling effect on the freedom of expression of ordinary citizens and a wide range of vulnerable groups.[652] Penney's research has suggested that chilling effects are greater with online surveillance as opposed to other regulatory actions and that women and younger people are more likely to be chilled and are less likely to take steps to defend themselves from regulatory actions and threats.[653] It has also been statistically demonstrated that Muslim-American's change their behaviour due to government surveillance fears.[654] Rozemarijn van der Hilst [655] and Jillian York[656] have both noted how wide-scale communications data retention can have a severe chilling on freedom of association 'which is

[647] PageFair, 'The state of the blocked web 2017 Global Adblock Report' (2017) <https://pagefair.com/downloads/2017/01/PageFair-2017-Adblock-Report.pdf> accessed 20 September 2017.
[648] Andrea Peterson, 'Why Edward Snowden thinks you should use an ad blocker' *The Washington Post* (Washington, D.C, 13 November 2015) <https://www.washingtonpost.com/news/the-switch/wp/2015/11/13/why-edward-snowden-thinks-you-should-use-an-ad-blocker/> accessed 20 September 2017.
[649] Rozemarijn van der Hilst, (n639), p20-21; German Forsa Institute, 'Meinungen der Bunderburger zur Vorratsdatanspeicherung' (2008) <http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf> accessed 11 March 2018.
[650] Lilian Mitrou, 'The Impact of Communications Data Retention on Fundamental Rights and Democracy — The Case of the EU Data Retention Directive in Kevin D. Haggerty and Minas Samatas (eds) *Surveillance and Democracy* (Routledge-Cavendish 2010), 127, 138.
[651] Valerie Aston, 'State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives' (2017) EJLT 8:1 <http://ejlt.org/article/view/548/730> accessed 28 April 2017.
[652] David Kaye, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (11 May 2016) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/12/PDF/G1609512.pdf?OpenElement> accessed 4 May 2017, para 57.
[653] Jonathon W. Penney, 'Internet surveillance, regulation, and chilling effects online: a comparative case study' (2017) Internet Policy Review 6:2; Jonathon W. Penney, 'Whose Speech Is Chilled by Surveillance?' (7 July 2017) <http://www.slate.com/articles/technology/future_tense/2017/07/women_young_people_experience_the_chilling_effects_of_surveillance_at_higher.html> accessed 17 August 2017.
[654] Dawinder S. Sidhu, 'The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim Americans' (2007) 7 U. Md. L.J. Race Relig. Gender & Class 375 7:2 <http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1134&context=rrgc> accessed 12 May 2017.
[655] Rozemarijn van der Hilst, 'Ranking, in terms of their human rights risks, the detection technologies and uses surveyed in WP09' (2011) <http://www.detecter.bham.ac.uk/pdfs/17_4_human_rights_ranking_of_technologies.doc> accessed 12 May 2017.
[656] Jillian York, 'The harms of surveillance to privacy, expression and association' (2014) <https://giswatch.org/en/communications-surveillance/harms-surveillance-privacy-expression-and-association> accessed 12 May 2017.

a loss for the democratic functioning of society.'[657] Manokha notes that since Snowden's revelations, there has been chilling effects in journalism, social media behaviour (online and offline), political opinions and identity expressions [658] The chilling effect on rights exercised under Articles 8-11 and Article 2 Protocol 4 can lead to what Tijmen Schep coins as 'social cooling' in which 'the long-term negative side effects of living in a reputation economy' because everything is remembered.[659]

Solove noted that the value of protecting against chilling effects is not measured simply by its effects on individuals exercising their rights, but its harms to society because among other things 'they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity.'[660] In addition to the severity of the interference with an individual's rights to privacy and data protection, it can also be argued that the changes in society, potentially resulting from a constant surveillance, are contrary to the public purpose.[661] Just as the ECtHR found violations of Article 10/11 in *Segerstedt-Wiberg and Others* [662] despite actual harm not being demonstrated.

b. Legal Professional Privilege/Journalistic Sources

As the DCH noted, data retention infringes upon Article 10 ECHR/Article 11 CFR due to the chilling effect of contact between journalists and source, and lawyers and clients,[663] and should thus be excluded.[664]

i. Legal Professional Privilege

As Chapter 4 noted, Lord Neuberger highlighted that:

> [I]t is self-evident that knowing that a consultation or the communication may be the subject of surveillance could have a chilling effect on the openness which should govern communications between lawyer and client.[665]

The Law Society and the Bar Council also raised concerns about data retention and LPP.[666] They noted that the problem bulk communications data retention is that it does not prevent LLP data from entering the 'pool' in the first place,[667] something which the CJEU also highlighted.[668] The Law Society and Bar Council considered that 'new legislation should prevent an obligation being placed on service providers *to retain data relating to*

[657] Rozemarijn van der Hilst, (n655).
[658] Ivan Manokha, 'Surveillance, Panopticism, and Self-Discipline in the Digital Age' (2018) Surveillance and Society 16:2 219, 229-230
[659] Tijmen Schep, 'Data Leads to Social Cooling' <https://www.socialcooling.com/> accessed 20 September 2017.
[660] Daniel J. Solove, ''I've Got Nothing to Hide' and Other Misunderstandings of Privacy' (2007) San Diego Law Review 44 745, 746.
[661] Lukas Feiler, (n511).
[662] *Segerstedt-Wiberg and Others*, (n375), [105], [107].
[663] Decision of the District Court of The Hague, (n436), [2.2].
[664] Opinion of Saugmandsgaard Øe, (n1), [212].
[665] *McE, Re* (Northern Ireland) [2009] UKHL 15, [111].
[666] Law Society and Bar Council, 'Investigatory Powers and Legal Professional Privilege' (2015) <https://www.lawsociety.org.uk/news/documents/position-paper-investigatory-powers-legal-professional-privilege-october-2015/> accessed 17 May 2017.
[667] ibid, para 32.
[668] *Digital Rights Ireland*, (n2), [57-8]; *Tele2 Sverige AB and Watson*, (n3), [105].

communications to or from users known to be professional legal advisers (author's emphasis).'[669] This was also the position of AG Saugmandsgaard Øe in *Tele2 and Watson*.[670] Jessica Sobey noted that '[k]nowing who a lawyer contacts, when the contact was made and even where the point of contact was in geographical terms at the time, can be enough to represent a material breach of privilege.'[671] This is all the more important considering that the accused's rights to communicate with his advocate out of hearing of a third person *is part of the basic requirements of a fair trial in a democratic society* (author's emphasis).[672]

ii. Journalistic Sources

Journalism is regarded as the 'fourth estate'[673] in which political reporting and investigative journalism attract a high level of protection under Article 10.[674] Protections, however, are uniquely challenged in the context of data retention.[675] Reporters Without Borders noted how the UK had slipped down World Press Freedom Index, with a reason being the adoption of the IPA 2016 which provided 'insufficient protection mechanisms for whistleblowers, journalists, and their sources, posing a serious threat to investigative journalism.'[676] The United Nations Educational, Scientific and Cultural Organization (UNESCO) published a report on protecting journalistic sources in the digital age.[677] The report highlighted that many countries examined in the study legal source protection frameworks were being actually or potentially jeopardised by mandatory data retention policies.[678] A key finding was that without substantial strengthening of legal protections and limitations on data retention, investigative journalism that relies on confidential sources will be difficult to sustain in the digital era, and reporting in many other cases will encounter inhibitions on the part of potential sources.[679] UNESCO highlighted that even when journalists encrypt the content, they may neglect to encrypt the communications data meaning they still leave behind a digital trail when they communicate with their sources which can easily identify a source,[680] such as Whatsapp usage.[681]

c. Anonymity

---

[669] Law Society and Bar Council, (n666), para 32.
[670] Opinion of Saugmandsgaard Øe, (n1), [212].
[671] Jessica Sobey, 'Legal professional privilege under fire' <http://www.stokoepartnership.com/wp-content/uploads/2016/06/Jessica-Sobey-Legal-Professional-Privilege-Under-Fire-CLJ-Vol.-180.pdf> accessed 17 May 2017.
[672] *S. v Switzerland* App nos. 12629/87 13965/88 (ECHR, 28 November 1981), [48].
[673] Sal Humphreys and Melissa de Zwart, 'Data retention, journalist freedoms and whistleblowers' (2017) Media International Australia 1–14, 1.
[674] *Mosely v UK* App no. 48009/08 (ECHR, 10 May 2011), [129].
[675] Sal Humphreys and Melissa de Zwart, (n673), 1-2.
[676] Reporters Without Borders, 'A worrying trend' <https://rsf.org/en/united-kingdom> accessed 17 August 2017; Chloe Farand, ''Worrying trend' of freedom of the press in the UK as country ranks 40 in latest Reporters Without Borders index' *The Independent* (London, 14 August 2017) <https://www.independent.co.uk/news/world/world-press-freedom-index-2017-reporters-without-borders-uk-freedom-information-a7893211.html> accessed 18 August 2017.
[677] Julie Posetti, 'Protecting Journalism Sources in the Digital Age' (2017) <http://www.wan-ifra.org/sites/default/files/field_message_file/248054E.pdf> accessed 18 August 2017.
[678] ibid, p7.
[679] ibid, p18
[680] ibid, p26.
[681] Aike Müller-Keezel, '3 potential holes in WhatsApp's end-to-end encryption' (4 May 2016) <https://venturebeat.com/2016/05/04/3-potential-holes-in-whatsapps-end-to-end-encryption/> accessed 18 August 2017.

Mitrou has argued that blanket data retention, by making communication activity potentially traceable, has a disturbing effect on the willingness to voice critical and constructive ideas, and on the free exchange of information and ideas, which is of paramount importance in a democratic society.[682] Catherine Crump has uttered similar remarks that since data retention would make all Internet activity traceable, its successful implementation would eliminate anonymity online which would be a regulation of unprecedented scope because it would eliminate the anonymity of those receiving information as well as those conveying information.[683] Additionally, it can have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimisation,[684] which could also undermine the ability to solve crime.[685] As Bernal maintains, strong anonymity is needed for whistleblowers,[686] especially when going to the press as a journalist source (as discussed above). Similarly, the Slovenian Constitutional Court noted that data retention disallows the anonymous use of means of communication for cases where the communication is confidential.[687] They continued that it was also incomprehensible for all those cases where the confidential and unpredictable use of means of communication is necessary in order to achieve its purpose (e.g. telephone assistance for help in mental distress).[688] The importance of anonymity becomes all the more pertinent when the IPA 2016 makes it possible to compel VPN's to keep logs via generating communications data.

d. Surveillance by Design

Chapter 3 and 6 demonstrated how the definition of telecommunications operator and communications data allowed retention notices to be issued on essentially anything that can communicate, whether it be a smart or IoT object to retain essentially any type of data including Big Data. The term 'Surveillance by Design' was first coined by Thani *et al*[689] and for the purposes of this thesis, it will be used in a different context. As Tijmen Wisman notes, it only takes a few tweaks to turn the IoT into an 'unprecedented surveillance-society.'[690] Wisman continued that if data retention is applied to the IoT (which it does under the IPA 2016), the 'amount of data and the level of detail will increase dramatically and will leave less space for citizens to keep information about their lives to themselves.'[691] Although Wisman refers to the IoT as purpose creep by design, it is argued that the concept of 'Surveillance by Design' is

[682] Lilian Mitrou, (n622), 427.
[683] Catherine Crump, 'Data Retention: Privacy, Anonymity, and Accountability Online' (2003) 56 Stan. L. Rev. 191, 216; see also Frank La Rue, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (17 April 2013) <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf> accessed 18 August 2017, para 49.
[684] Frank La Rue, (n683), para 24.
[685] Joint Committee on the Draft Investigatory Powers Bill, *oral evidence*, (n256), Caroline Wilson Palow, answer to Q130.
[686] Paul Bernal, (n42), 238-9.
[687] The Constitutional Court of the Republic of Slovenia, U-I-65/13-19 of 3 July 2014, [25].
[688] ibid.
[689] Sharifah Khalizah Syed OthmanThani, Nor Hanisah Mohd. Hashim and Wan Hazwatiamani Wan Ismail, 'Surveillance by Design: Assessment using principles of Crime Prevention through Environmental Design (CPTED) in urban parks' (2016) Elsevier Procedia - Social and Behavioral Sciences 234 506.
[690] Tijmen Wisman, 'Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things' (2013) European Journal of Law and Technology 4:2 <http://ejlt.org/article/view/192/379> accessed 1 September 2017.
[691] ibid.

more appropriate in this context because the IoT *is* surveillance[692] and if the State can compel the retention of such data generated by IoT objects, it only marks a *shift* in *who* is conducting the surveillance. Thus, this highlights that the IoT will feed 'into the surveillance apparatus of the state'[693] whether it is outside, one's home or *within* creating a God's-eye view of ourselves.[694]

i. Data Retention makes your City a Panopticon

The IoT will extend in the form of Smart Cities.[695] The Economist highlighted that clever cities may not be better ones and rather than becoming paragons of democracy, they could turn into electronic Panopticons in which everyone is watched,[696] destroying the sense of privacy and urban anonymity.[697] Rob Kitchin, referring to Solove's taxonomy of privacy, noted that the 'vast quantity of highly detailed spatial behaviour data from which lots of other insights can be inferred (such as mode of travel, activity, and lifestyle)' from smart cities.[698] The consequences is that individuals are no longer lost in the crowd but 'are being tracked and traced at different scales of spatial and temporal resolution.'[699] This demonstrates the interferences particularly with Article 2 Protocol 4 and Article 11 given that tracking takes place with no attempt at consent, often with little notification and with no ability to opt-out.[700] As Valerie Aston noted that surveillance undermines some of the key building blocks of successful mobilisations.[701] It was argued that although as Aston rightly suggests, the UK courts have not adequately protected Article 8 and 11 regarding public space surveillance, with regards to smart cities, the situation, however, changes[702] as this involves the systemic collection of data (personal and sensitive), thus the chilling effect[703] intensifies.

Smart cities can demonstrate how Bentham's Panopticon is 'child's play compared to surveillance in a fully functioning IoT.'[704] As Wisman continues that 'if society is constructed

[692] J.M. Porup, 'The Internet of Things is a surveillance nightmare' (20 March 2016) <http://kernelmag.dailydot.com/issue-sections/staff-editorials/16196/internet-of-things-surveillance-nightmare/> accessed 3 September 2017.
[693] Tijmen Wisman, (n690).
[694] Alex Pentland, 'Society's Nervous System: Building Effective Government, Energy, and Public Health Systems' (2012) IEEE Computer Society 39, 45.
[695] Felix Wortmann and Kristina Flüchter, 'Internet of Things - Technology and Value Added' (2015) Bus Inf Syst Eng 57:3 221, 222; Ed Vaizey, 'Manchester wins £10m prize to become world leader in 'smart city' technology' (3 December 2015) <https://www.gov.uk/government/news/manchester-wins-10m-prize-to-become-world-leader-in-smart-city-technology> accessed 2 September 2017.
[696] The Economist, 'Clever cities The multiplexed metropolis' *The Economist* (London, 5 September 2013) <https://www.economist.com/news/briefing/21585002-enthusiasts-think-data-services-can-change-cities-century-much-electricity?frsc=dg/a> accessed 2 September 2017.
[697] Kelsey Finch and Omer Tene, 'Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town' (2015) Fordham Urban Law Journal 41:5 1581, 1582.
[698] Rob Kitchin, 'Getting smarter about smart cities: Improving data privacy and data security' (2016) <http://www.taoiseach.gov.ie/eng/Publications/Publications_2016/Smart_Cities_Report_January_2016.pdf> accessed 2 September 2017, p33.
[699] ibid.
[700] ibid, p38.
[701] Valerie Aston, 'State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives' (2017) EJLT 8:1 <http://ejlt.org/article/view/548/730> accessed 28 April 2017, 9.
[702] See Chapters 4 and 6.
[703] Valerie Aston, (n701), 9, 12 and 14.
[704] Tijmen Wisman, (n690).

in a way that every act of the individual causes the processing of data that is captured in databases accessible by public authorities, the principle of proportionality is neglected.'[705]

ii. Data Retention makes your Home your own Personal Panopticon

It was highlighted that the 'home' and 'family life' aspects of Article 8 even more imperative when it came to data retention. It also turned Sir Edward Coke's maxim on its head as the IPA 2016 would no longer make a man's home his castle, turning it into his own personal Panopticon. An example of this is the case of *R. v. Orlandis-Habsburgo* in which the appellant's energy provider were able to detect a pattern of electricity use in the residence that was consistent with the operation of a marijuana grow-op,[706] using smart meter technology.[707] Under the IPA 2016, or even the DRD[708] this could be retainable as for e.g. entity data and thus demonstrates the amount of insight into one's home that can be gained from a retention notice. As Colette Cuijpers and Bert-Jaap Koops notes, smart meters potentially constitute a breach of the right to inviolability of the home and the right to family life.[709] This is due to the fact that smart meters allow via a wall socket – to look 'behind the front door' with great precision giving grid managers and suppliers of gas and electricity will obtain information about such things as lifestyles, holidays, the types of electronic products present,[710] and health professionals, health indicators.[711] Baroness Hale in *Countryside Alliance* highlighted the separate but related fundamental values of 'the inviolability of the home and personal communications from official snooping.'[712] As the IoTs (particularly home devices) poses a 'serious threat to privacy'[713] these two fundamental values are going to become more aligned than they ever have. Moreover, smart meters are a new example of technology that makes it possible to see from the outside what takes place inside homes and, all things considered, turns it into the proverbial glass house,[714] which can have a chilling effect on indoor activities/relationships.[715]

Although Colette Cuijpers and Bert-Jaap Koops's study concerned compulsory use of smart meters, that was only one of three reasons[716] why they felt it was not necessary in a democratic

---

[705] ibid.
[706] *R. v. Orlandis-Habsburgo*, 2017 ONCA 64, [1].
[707] ibid, [11].
[708] Tijmen Wisman, (n690).
[709] Colette Cuijpers and Bert-Jaap Koops, 'The 'smart meters' bill: a privacy test based on article 8 of the ECHR' (October 2008) <https://skyvisionsolutions.files.wordpress.com/2014/11/dutch-smart-meters-report-tilt-october-2008-english-version.pdf> accessed 20 August 2017, p21.
[710] ibid, p3-4.
[711] Louise Rogerson, 'How a smart meter could save your life' *The Spectator* (18 July 2018) <https://health.spectator.co.uk/how-a-smart-meter-could-save-your-life/?_lrsc=dbc7fdf0-368e-4711-9bae-da8fa3fa3d4b&_lrsc=cf7b4f02-2490-43e2-98c6-d075e421c98c> accessed 30 July 2018.
[712] *Countryside Alliance and others, R (on the application of) v Attorney General & Anor* [2007] UKHL 52, [116].
[713] Glynn Moody, 'Welcome to the Internet of listening, eavesdropping, spying things' (25 August 2017) <https://www.privateinternetaccess.com/blog/2017/08/welcome-internet-listening-eavesdropping-spying-things/>
[714] Colette Cuijpers and Bert-Jaap Koops, (n709), p22.
[715] ibid, p21.
[716] The hourly/quarter hourly and daily readings were also deemed disproportionate.

society.[717] They also raise consent issues under the GDPR.[718] Smart meters are but one example of the increasing transparency of our home and careful consideration of the cumulative effect of the various developments that allow insight into how people live, in the one place where people most of all must feel free to do what they like because if our home will no longer be our castle, the house may be energy-efficient but it will be a cold place to live.[719]

iii. Data Retention makes YOU the Panopticon

Kelsey Finch and Omer Tene highlight that linking the human body with its physical, behavioural and psychological individuality to a government managed grid raises concerns about privacy, surveillance, control, and chilling effects.[720] Chapter 6 highlighted that wireless body area networks WBAN which would fall under the definition of telecommunications operator, thus whoever controls it could have a retention notice issued on them. There is already an example of WBAN data being used in criminal matters. In the US where a Butler County, Ohio Judge ruled that data from a suspect's own pacemaker could be used against them as evidence.[721]

Chapter 6 noted that those who provide or control wearable tech[722] would also fall under the definition of telecommunications operator. This is a form of sousveillance[723] (inverse surveillance[724] where the user becomes the observer)[725] in which data is shared with the manufacturers and often others.[726] Therein lays the danger as the communications data generated by such technology is not decentralised (no centralised database of privacy sensitive data)[727] and thus still readily available for retention. For this reason, Mateusz Bucholski argued that sousveillance and surveillance are two sides of the same coin because they *both* infringe upon individual freedom.[728] Chapter 3 already noted how Facebook is seeking to develop

---

[717] Colette Cuijpers and Bert-Jaap Koops, (n709), p36; K.T. Weaver, 'Dutch case study: "smart" meter privacy invasions are unjustifiable in a democratic society' (6 November 2016) <https://takebackyourpower.net/smart-meter-privacy-invasions-are-unjustifiable-in-a-democratic-society/> accessed 20 August 2017.
[718] Cristina Ulessi, 'France: CNIL's notice to DIRECT ENERGIE on collection of smart meter data "indication of likely approach of DPAs post-GDPR"' (29 March 2018) <https://www.dataguidance.com/france-cnil-notice-direct-energie-collection-smart-meters-data-indication-likely-approach-dpas-post-gdpr/> accessed 1 Augsut 2018.
[719] Colette Cuijpers and Bert-Jaap Koops, 'Smart metering and privacy in Europe: lessons from the Dutch case' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds) *European Data Protection: Coming of Age* (Springer 2012).
[720] Kelsey Finch and Omer Tene, (n697), 1601-2.
[721] Chris Matyszczyk, 'Judge rules pacemaker data can be used against defendant' (12 July 2017) <https://www.cnet.com/news/judge-rules-pacemaker-data-can-be-used-against-defendant/?ftag=COS-05-10aaa0b&linkId=39705414> accessed 25 August 2017.
[722] Kelsey Finch and Omer Tene, (n697), 1600.
[723] Rob Kitchin, 'Continuous Geosurveillance in the "Smart City"' <http://dismagazine.com/dystopia/73066/rob-kitchin-spatial-big-data-and-geosurveillance/> accessed 4 September 2017.
[724] Steve Mann, 'Sousveillance, not just surveillance, in response to terrorism' (2002) Metal and Flesh 6:1 <http://wearcam.org/metalandflesh.htm> accessed 4 September 2017.
[725] Mateusz Bucholski, 'Surveillance and sousveillance on Facebook: Between empowerment and disempowerment' (2016) MaRBLE Research Papers Vol III, 22.
[726] Rob Kitchiin, (n723).
[727] Bart Jacobs, 'Keeping our Surveillance Society Nontotalitarian' (2009) Amsterdam Law Forum 1:4 <http://amsterdamlawforum.org/article/view/91/165> accessed 4 September 2017.
[728] Mateusz Bucholski, (n725), p23.

technology that would be able to read a person's mind in order to communicate,[729] thus allowing Facebook the potential to collect data on our very thoughts.[730] This data could then be retainable and would truly encompass what Caspar Bowden highlighted when he coined the term 'CCTV for inside your head'[731] with respect to data retention. This would amount to the greatest of threats to freedom of thought and conscious protected by Article 9 and autonomy in general. As Chapter 4 noted, the mind is a 'kind of last refuge of personal freedom and self-determination.'[732] Moreover, Chapter 4 demonstrated how privacy of the mind could be interfered with by neurotechnologies and have Article 9 implications (which the manifestation is absolute). Marcello Ienca and Roberto Andorno argues that a new right to brain privacy should be adopted which would protect against 'illegitimate access to their brain information and to prevent the indiscriminate leakage of brain data across the infosphere.'[733] They continued that violations of mental privacy can occur when *brain data* is *collected* for research purposes are stored on external databases and where brain data generated by consumer-grade brain-computer interfaces (BCI) are sent to a connected app and can be stored in the cloud or other data store end points.[734]

If neurotechnologies can be used to discern the contents of thoughts against one's will (non-consent)[735]'it would have a chilling effect not only on expression but also on the source of expression, and thus it would impact the freedom people have even to entertain those thoughts.'[736] Neurotechnologies creates risk of unparalleled intrusion into the private sphere causing physical or psychological harm or unduly influencing one's behaviour.[737] The very notion of freedom of thought could very well be put under threat as retention of thought data could be seen as taking 'coercive steps to make him change his beliefs.'[738] Chapter 4 concluded that privacy of the mind is best protected under Article 9 due to its absolute nature to protect freedom of thought and conscious.

e. The Cyclical Nature of Retention, a Continuous Violation

Section 87(3) of the IPA 2016 allows data to be retained for up to retained for 12 months. It was already noted above that pressing social need for this 12-month period had not been made. Furthermore, it was also noted that even six months of irrelevant (which is most retained data)

---

[729] Olivia Solon, 'Facebook has 60 people working on how to read your mind' *The Guardian* (London, 19 April 2017) <https://www.theguardian.com/technology/2017/apr/19/facebook-mind-reading-technology-f8> accessed 24 April 2017.
[730] Aatif Sulleyman, 'Facebook could farm users' thoughts with Mind-Reading technology to sell adverts' *The Independent* (London, 25 May 2017) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-mind-reading-technology-thoughts-sell-adverts-social-media-accounts-a7755136.html> accessed 4 September 2017.
[731] Caspar Bowden, 'CCTV for inside your head Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation' (2001) <http://europe.rights.apc.org/eu/cctv_for_the_head.html> accessed 24 April 2017.
[732] ibid, 1.
[733] Marcello Ienca and Roberto Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology' (2017) Life Sciences, Society and Policy 13:5 1, 15.
[734] ibid.
[735] Stephen Mumford and Rani Lill Anjum, 'Powers, Non-Consent and Freedom' (2014) Philosophy and Phenomenological Research 91:1 136.
[736] Adina L. Roskies, 'Mind Reading, Lie Detection, and Privacy' in Jens Clausen and Neil Levy (ed), *Handbook of Neuroethics* (Springer Netherlands 2015), 687.
[737] Marcello Ienca and Roberto Andorno, (n733), 2.
[738] *Ivanova v Bulgaria* App no. 52435/99 (ECHR, 12 April 2007), [79].

communications data storage could not be justified. Another problem is because every time communications data is created, the 12-month time limit starts again. This highlights a never-ending interference irrespective of whether data is destroyed. In a sense, communications data retention is indefinite because of the continued indiscriminate nature. The very premise of the 12-month period appears circular in effect, because although that *specific* communications data has been destroyed, this has no overall effect on the continuing communications data retention.

The RCC highlighted this point in that the continuous character of retention derogates from the principle of personal data protection and their confidentiality by emptying the content of this principle. In this regard, the RCC also referred again to ECtHR jurisprudence in that Member States' guarantee of rights must be practical and effective, not theoretical and illusory as 'the continuous retention of personal data transforms…the exception from the principle of effective protection of privacy right and freedom of expression, into an absolute rule.[739] The RCC also noted that the continuous limitation of rights makes the essence of it disappear by removing the safeguards regarding its execution. They continued that physical, legal persons and mass users of services would become permanent subjects of intrusions into the exercise of their privacy of correspondence, freedom of expression 'without the possibility of a free, uncensored manifestation, except for direct communication, thus excluding the main communication means used.'[740] The RCC also levied criticism at the fact that 'intrusion into the free exercise of the right takes place continuously and independently of the occurrence of a justifying fact, of a determinant cause.'[741]

The ECtHR also acknowledge '[t]he doctrine of "continuing violation" [which] implies a beginning, i.e., a critical event constituting the original breach, and its continuation.'[742] Judge Pettit in *Malone* noted that it was just as serious to be subject to surveillance as to be unable to stop it when they are illegal and unjustified 'as was for example the case with Orwell's character who, *within his own home, was continually supervised by a television camera without being able to switch it off* (author's emphasis).'[743]

f. Safeguards: Judicial Oversight is Insufficient

The HC refers to the JC's role in retention notices and the fact that s.2 of the IPA 2016 and the general duties of JC's in relation to privacy and the protection of sensitive information.[744] This Chapter has highlighted the many ways in which data retention under the IPA 2016 violates a collection of Convention Rights and it has been noted that 'transferring the power to issue said notice (in the UK's case, a JC or IPC) would still not create a Convention compliant'[745] system. This is because the problems highlighted above[746] still persist and the JC system would still wield a virtually unfettered power.[747] Moreover, when considering adequate safeguards, the ECtHR looks to the independence of the authorisation authority.[748] It has already been argued

[739] Romania Constitutional Court, (n148).
[740] ibid.
[741] ibid.
[742] *Loizidou v Turkey* App no. 15318/89 (ECHR, 28 July 1998), Dissenting Opinion of Judge Jambrek, [5].
[743] *Malone v UK* App no. 8691/79 (ECHR, 2 August 1984), Concurring Opinion of Judge Pettiti.
[744] *Liberty* (n99), [133-135].
[745] Matthew White, (n4), 37.
[746] See section 7.3B(2)(i)(a).
[747] Matthew White, (n4), 38.
[748] *Roman Zakharov*, (n6), [278-80].

that the JC and IPC does not establish sufficient independence[749] from the executive[750] and themselves.[751]

The IPC released an advisory notice (which has now been removed) for JCs, public authorities and the public on authorisations, warrants and notices.[752] The advice entails that when a JC considers a retention notice, they must have due regard to the general privacy duties set out in s.2 of the IPA 2016,[753] the relevant tests of necessity and proportionality under ECHR and EU law,[754] and where fundamental rights are engaged the *Wednesbury* principles will not be applied.[755] These safeguards and more, however, are undermined by the fact that the notice is only advisory, and admits it lacks a binding nature,[756] contrary to the ECHR[757] and EU law.[758]

Moreover, confining the JC's role in s.2 of the IPA 2016 to consider privacy, overlooks other fundamental rights[759] mentioned in this Chapter. With regards to the protection of sensitive information, this is much narrower than what is considered sensitive personal data in data protection instruments, and in any event would not protect against communications data from the result of communications with journalists and sources, lawyers and clients.[760]

g. Crime

Due to the IPA 2016 not defining crime, this creates a problem as '"[c]rime" can of course include trivial offences, and only the requirements of necessity and proportionality can prevent communications data being used for such crimes.'[761]

h. Alternatives to Data Retention

Data preservation was discussed in some detail above. Kristina Ringland noted, data preservation '*achieves a better balance* between assisting law enforcement in criminal investigations while minimizing the costs to both corporations and consumers (author's emphasis).'[762]

i. Security Risks

---

[749] ibid, [302].
[750] Matthew White, (n4), 17, 32-3.
[751] ibid, 32.
[752] Investigatory Powers Commissioner Office, 'Approval of Warrants, Authorisations and Notices by Judicial Commissioners' (March 2018) <http://www.ipco.org.uk/docs/20180308_IPCO%20Advisory%20Notice%2012018.pdf> accessed 13 March 2018.
[753] ibid, para 16.
[754] ibid, para 17.
[755] ibid, para 19.
[756] ibid, para 1.
[757] *Valenzuela Contreras*, (n150), [60]; 'For this purpose, the rules need not be statutory, provided that they operate within a framework of law and that there are effective means of enforcing them.' *Catt and T, R (on the applications of) v Commissioner of Police of the Metropolis* [2015] UKSC 9, [11].
[758] Opinion of Saugmandsgaard Øe, (n1), [150]; *Tele2 Sverige AB and Watson*, (n3), [117].
[759] Matthew White, (n4), 28-29.
[760] Matthew White, (n102).
[761] Joint Committee on the Draft Communications Data Bill, (n45), para 141.
[762] Kristina Ringland, 'The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model' (2009) SHIDLER J. L. COM. & TECH 5:3.

The risks of communications data retention have been noted by many.[763] Colette Cuijpers and Bert-Jaap Koops noted security risks of smart meters which could allow burglars to threaten the inviolability of the home.[764] As noted, in 2014, 90% of large firms, and 74% of small firms in the UK suffered a security breach.[765] Even telecommunications operators such as TalkTalk,[766] Three,[767] Vodafone,[768] Time Warner Cable,[769] energy companies,[770] credit firms,[771] and even the CIA[772] were victims of security breaches.

Section 92 of the IPA 2016 deals with data security. Section 92(1)(a) compels the telecommunications operator to secure data to the same level they normally would. This, in and of itself does not guarantee high data security standards. Section 92(1)(c) replicates the information security principles of the Data Protection Act 1998, but as the GFCC noted when referring their domestic data protection legislation in that it was 'too general to ensure in a sufficiently specific and reliable manner the particularly high security standards with regard to the data to be stored.'[773] Danny O'Brien notes that 'the best form of data security is simply not collecting that information in the first place.'[774] Data retention is the opposite of data protection as it raises the chances of catastrophic losses of privacy with no benefit for the people it endangers.[775]

This problem intensifies with smart cities as Rob Kitchin noted that:

---

[763] Joint Committee on the Draft Investigatory Powers Bill, *written evidence*, (n43), Zara Rahman, para 4, p1180, Paul Bernal, para 8, p139-140; Joint Committee on the Draft Investigatory Powers Bill, (n45), para 31, paras 164-167; Science and Technology Committee, (n166), para 57.
[764] Colette Cuijpers and Bert-Jaap Koops, (n709), p21; Colette Cuijpers and Bert-Jaap Koops, (n719).
[765] Joint Committee on the Draft Investigatory Powers Bill, (n45), para 166.
[766] Leo Kelion, 'TalkTalk's wi-fi hack advice is 'astonishing'' *BBC News* (London, 7 December 2016) <http://www.bbc.co.uk/news/technology-38223805> accessed 21 August 2017.
[767] Robert Booth, 'Three UK's mobile customers experience new data breach' *The Guardian* (London, 20 March 2017) <https://www.theguardian.com/business/2017/mar/20/three-mobile-possible-data-breach-data-usage-call-history> accessed 21 August 2017.
[768] Press Association, 'Vodafone customers' bank details 'accessed in hack', company says' *The Guardian* (London, 31 October 2015) <https://www.theguardian.com/business/2015/oct/31/vodafone-customers-bank-details-accessed-in-hack-company-says> accessed 21 August 2017.
[769] Giovanni Bruno and Chris Nolter, 'Millions of Time Warner Cable Customers' Information Exposed' (1 September 2017) <https://www.thestreet.com/story/14291954/1/millions-of-time-warner-cable-customer-s-information-exposed-after-data-leak.html> accessed 8 September 2017.
[770] Alex Hern, 'State hackers 'probably compromised' energy sector, says leaked GCHQ memo' *The Guardian* (London, 18 July 2017) <https://www.theguardian.com/technology/2017/jul/18/energy-sector-compromised-state-hackers-leaked-gchq-memo-uk-national-cybersecurity-centre> accessed 21 August 2017; Cara McGoogan, 'Hackers targeting UK energy grid, GCHQ warns' *The Telegraph* (London, 18 July 2017) <http://www.telegraph.co.uk/technology/2017/07/18/hackers-targeting-uk-energy-grid-gchq-warns/> accessed 21 August 2017.
[771] Olivia Solon, 'Credit firm Equifax says 143m Americans' social security numbers exposed in hack' *The Guardian* (London, 8 September 2017) <https://www.theguardian.com/us-news/2017/sep/07/equifax-credit-breach-hack-social-security> accessed 8 September 2017.
[772] George Danezis, 'What the CIA hack and leak teaches us about the bankruptcy of current "Cyber" doctrines' (8 March 2017) <https://www.benthamsgaze.org/2017/03/08/what-the-cia-hack-and-leak-teaches-us-about-the-bankruptcy-of-current-cyber-doctrines/> accessed 21 August 2017.
[773] BVerfG, (n176), [274].
[774] Danny O'Brien, 'Data Privacy Means Data Security (and not Data Retention)' (27 January 2014) <https://www.eff.org/deeplinks/2014/01/data-privacy-means-data-security-and-not-data-retention> accessed 21 August 2017.
[775] ibid.

> Research by cybersecurity specialists has discovered that many smart city systems have been constructed with no or minimal security and city governments and vendors are deploying them without undertaking cybersecurity testing.[776]

Lilian Edwards noted that in short 'smart cities are a security disaster waiting to happen.'[777] Security threats also persist with brain/mind data as Ajaya Neupane, Lutfor Rahman and Nitesh Saxena demonstrated that passwords and PINs could be predicted based on brain signals which as noted above, such signals could be retained with neurotechnologies.[778]

Conclusions

The above subsection has demonstrated why a fair balance could never be struck regarding data retention as envisaged in the IPA 2016. The authorisation procedures are not capable of ensuring that secret surveillance measures are ordered only when 'necessary in a democratic society.'[779] This conclusion obviates the need to consider criticisms of the 'adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data.'[780] Therefore, even *if* the JC system was an adequate safeguard, the scale and generality of retention would make this inconsequential to the violations of Articles 8-11 and Article 2 Protocol 4.

7.7. Data Protection

a. A Fundamental Right in itself

Fuster has argued that the CJEU's case law on personal data protection when privacy is involved has been confusing as to how the two rights relate and whether they should be relied upon separately and how they are lawfully restricted.[781] Although the ECHR has no Article 8 CFR equivalent,[782] the interpretation of Article 8 ECHR has been directly influenced by the emergence and development of data protection concepts and laws,[783] as seen in *S and Marper*.[784] The GC in *S and Marper* recognised how fundamental the protection of personal data was to the enjoyment of Article 8 ECHR, and that domestic law must afford appropriate

---

[776] Rob Kitchin, (n698), p39.
[777] Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective' (December 2015) <https://zenodo.org/record/34501/files/CREATe-Working-Paper-2015-11.pdf> accessed 1 August 2018.
[778] Ajaya Neupane, Lutfor Rahman and Nitesh Saxena, 'PEEP: Passively Eavesdropping Private Input via Brainwave Signals' (2017) <https://info.cs.uab.edu/saxena/docs/nrs-fc17.pdf> accessed 5 September 2017; Charlie Osborne, 'How hackers can hijack brainwaves to capture your passwords' *ZDNet* (8 May 2017) <http://www.zdnet.com/google-amp/article/how-hackers-use-brainwaves-to-capture-your-passwords/?utm_content=buffer5b8d1&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer > accessed 5 September 2017; Tom Simonite, 'Using Brainwaves to Guess Passwords' (5 May 2017) <https://www.technologyreview.com/s/604293/using-brainwaves-to-guess-passwords/?set=604330> accessed 5 September 2017.
[779] *Roman Zakharov*, (n6), [302].
[780] *S and Marper*, (n107), [125].
[781] Gloria González Fuster, (n36).
[782] Theodore Konstadinides, 'Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem' (2011) E.L. Rev. 36:5 722, 726.
[783] Sophie Stalla-Bourdillon, 'The Davis judgement: does Article 8 of the European Charter go beyond Article 8 of the ECHR?' (25 July 2015) <https://inforrm.wordpress.com/2015/07/25/the-davis-judgement-does-article-8-of-the-european-charter-go-beyond-article-8-of-the-echr-sophie-stall-bourdillon/> accessed 22 August 2017.
[784] *S and Marper*, (n107), [103].

safeguards that are *consistent* with it.[785] The CJEU in *Schecke* also noted that Article 7 and 8 CFR corresponded to Article 8 ECHR.[786] Although this poses its own problems,[787] this section will demonstrate how Article 8 ECHR can inform Article 8 CFR in the specific context of data retention because 'legislation limiting the right to the protection of personal data in compliance with Article 8 of the Charter may nevertheless be regarded as constituting a disproportionate interference with Article 7 (right to privacy) of the Charter.'[788]

b. Fair and Lawful Processing

Article 8(2) CFR notes amongst other things, that personal data must be processed fairly with consent or by some legitimate basis in law. Careful scrutiny must be taken when a measure authorises retention without consent.[789] Fair and lawful processing can be found within many data protection legal texts. also, known as the First Data Protection Principle.[790] It has been argued that lawful processing should be assessed 'in the context of compliance or non-compliance with the obligation to show'[791] respect for Article 8 of the ECHR. In *Law Society et all v Kordowski*, Tugendhat J noted that:

> [W]here the DPA applies, if processing is unlawful by reason of it breaching the general law of confidentiality *(and thus any other general law) there will be a contravention of the First Data Protection Principle* (author's emphasis). [792]

Tugendhat J also noted the link between Directive 95/46/EC and Article 8 ECHR.[793] A further link to human rights in general and data protection can be found in Recital 73 Regulation (EU) 2016/679 (GDPR). In an Enforcement Notice issued by the Information Commissioner's Office (ICO) on Southampton City Council, the ICO noted that '[a] breach of Article 8 [ECHR] will also contravene the lawful processing requirement of the First Data Protection Principle.'[794] An automatic number plate recognition (ANPR) system which took every number plate entering and leaving Royston[795] breached the First Data Protection Principle when taking into account Article 8 ECHR, for being unlawful and excessive.[796] Furthermore, processing

[785] ibid.
[786] Case C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, [52].
[787] Gloria González Fuster, (n36), 267-272; Rosanne Fleur Tijhaar, 'Data retention and the right to privacy, happily ever after? What the European Court of Justice and European Court of Human Rights teach us' (May 2018) <http://arno.uvt.nl/show.cgi?fid=145932> accessed 10 October 2018, 29.
[788] Opinion of Cruz Villalón, (n471), [61].
[789] *S and Marper*, (n107), [104].
[790] Article 5(a) of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981 (Convention 108), Article 5(1)(a) of Regulation (EU) 2016/679 and Article 6(1)(a) of Directive 95/46/EC.
[791] Chris Pounder, 'Information Commissioner should enforce Article 8 privacy rights' (20 April 2010) <http://amberhawk.typepad.com/amberhawk/2010/04/information-commissioner-should-enforce-article-8-privacy-rights.html> accessed 22 August 2017.
[792] *The Law Society, Hine Solicitors and Kevin McGrath v Rick Kordowski* [2011] EWHC 3185 (QB), [100].
[793] ibid, [97].
[794] ICO Enforcement Notice (23 July 2012) <http://breachwatch.com/wp-content/uploads/2012/08/Southampton-County-Council-Enforcement-Notice.pdf> accessed 22 August 2017, para 9.
[795] ICO Enforcement Notice (15 July 2013) <http://breachwatch.com/wp-content/uploads/2013/07/hertfordshire-constabulary-enforcement-notice.pdf> accessed 22 August 2017, para 3.
[796] ibid, para 7-8.

personal data has to be necessary on specified grounds.[797] Pounder has argued that where surveillance is unnecessary, this too can breach the First Data Protection Principle.[798]

This demonstrates that if a measure is unlawful under Article 8 ECHR where personal data is processed, this would also violate the lawful and fairness requirement. Sections 7.4 and 7.6 argued how data retention under the IPA 2016 was not in accordance with the law or necessary in a democratic society, and therefore, as this would breach the First Data Protection Principle, Article 8(2) and Article 52(1)[799] CFR would also be breached (excluding national security grounds). This too would be the case as not only is personal data processed, but sensitive personal data, which would in any case require stricter justifications for processing.[800] In terms of legality, this would also solve the tautologically trap of regarding a legal norm, the validity of which is being questioned, as being allegedly in accordance with the law because it is a law[801] if provided by law is equal to in accordance with.

c. Purpose Limitation

This is the Second Data Protection Principle which requires data must be collected for 'specified, explicit and legitimate' purposes (purpose specification) and not be 'further processed in a way incompatible' with those purposes (compatible use).[802] The ECtHR has noted where data protection issues under Article 8 arise, appropriate and adequate safeguards which reflect the principles elaborated *in applicable data protection* instruments and prevent arbitrary and disproportionate interference with Article 8 rights must be in place.[803]

The WP29 have noted that a purpose that is vague or general would not usually meet the criteria of being specific.[804] Section 7.4(B)(2)(i) noted how many of the purposes i.e. s.61(7) IPA 2016 were vague, and not, therefore, foreseeable, specific or explicit. WP29 also gave the example of the DRD which allowed processing for a clear incompatible purpose.[805] The WP29 continued this is further exasperated by the fact that citizens do not reasonably expect their communications data to be retained for law enforcement purposes, this data was not provided for (no consent), the confidentiality of the data, the volume of the data retained and the potential

[797] See generally Schedule 2 of the DPA 1998, Article 7 of Directive 95/46/EC and Article 6 of the GDPR; Article 29 Working Party, (n293), para 5.3.
[798] Chris Pounder, 'Nine principles for assessing whether privacy is protected in a surveillance society' (2008) IDIS 1:1 1, 3; Chris Pounder, 'Information Commissioner's enforcement proceedings links Article 8 to unlawful processing' (8 November 2012) <http://amberhawk.typepad.com/amberhawk/2012/11/information-commissioners-enforcement-proceedings-links-article-8-to-unlawful-processing.html> accessed 22 August 2017.
[799] Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.
[800] *S and Marper*, (n107), [103]; Article 29 Working Party, 'Advice paper on special categories of data ("sensitive data")' (4 April 2011) <http://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf> accessed 22 August 2017, p4-5.
[801] Gloria González Fuster, (n36), p271.
[802] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (2 April 2013) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 22 August 2017, p3-4.
[803] *M.M. v UK*, (n124), [195]. Note the applicable data protection instruments included among others, Article 8 CFR, GDPR, Directive 95/46/EC, Convention 108 and Committee of Ministers Recommendations [122-148].
[804] Article 29 Working Party, (n802), p15.
[805] ibid, p67-8.

consequences (criminal prosecution).[806] The WP29 noted that although the DRD had been legitimised, its foreseeability, necessity and proportionally was a matter for the CJEU[807] in which was found to not be the case for the reasons of necessity and proportionality. This Chapter adds to this finding whilst also demonstrating that foreseeability has also not been satisfied, and thus, the specified purpose under Article 8(2) CFR has not been complied with.

This is another important point to note, further processing for a different purpose does not necessarily mean that it is automatically incompatible.[808] Retention and access to communications data have the same purposes, however, nowhere in the IPA 2016 forbids retention for one purpose and accessing the same communications data for another. This question was put to Ben Emmerson QC and Helen Mountfield, who noted that there is a significant risk of a violation of Article 8 ECHR if communications data was not accessed for a business or national security purpose.[809] This would also be a *prima facie* breach of the First[810] and Second[811] Data Protection Principles, especially since communications data might contains sensitive personal data which would therefore narrow the scope for compatible use.[812] Would this require duplication of retained communications data to satisfy purpose limitation? Would this not create an even greater disproportionate interference with fundamental rights?

d. Relevant and Excessive

This is not specifically mentioned in Article 8(2) CFR but would be inherent in Article 8(1) in that everyone has the right to the protection of their personal data. In *S and Marper* the GC noted that domestic law should ensure that data are relevant and not excessive in relation to the purposes for which they are stored.[813] This is the Third Data Protection Principle and a similar position is taken by the EU[814] and CoE.[815] It was noted above that not only is most communications data irrelevant for the purposes for which they are retained, the amount retained was neither necessary or proportionate.

e. Accuracy

The Fourth Data Protection Principle requires data to be kept up to date and *accurate*. Feiler noted that due data retention creating the 'needle in the haystack problem' of detecting vaguely defined behaviours, it becomes prone to false positives and negatives.[816] A 'false positive' signifies an individual who is incorrectly identified as a 'terrorist' and a 'false negative' signifies a terrorist incorrectly identified as 'not a terrorist.'[817] Using the DRD as an example, and the EU population, Feiler noted that data mining and profiling would accurately identify 99

[806] ibid, p68.
[807] ibid.
[808] ibid, p21.
[809] Ben Emmerson QC and Helen Mountfield's Opinion to the ICO (19 June 2002) <https://www.whatdotheyknow.com/request/127491/response/315758/attach/html/3/Counsels%20Opinion%20re%20The%20Telecommunications%20Regulations%201999%2019.6.02.pdf.html> accessed 22 August 2017, para 13.4(b).
[810] ibid, para 9.7
[811] ibid, para 9.9.
[812] Article 29 Working Party, (n802), p25.
[813] *S and Marper*, (n107), [103].
[814] Article 6(c) of Directive 95/46/EC and Article 5(c) of the GDPR.
[815] Article 5(c) of Convention 108.
[816] Lukas Feiler, (n511).
[817] ibid.

terrorists for every 5 million that are incorrectly identified.[818] False positives and negatives were also highlighted by Manon Oostveen who went further and noted that in light of Big Data (discussed below) noted that risks of overfitting (mistaking coincidental patterns for patterns that are generalizable) are high.[819] This not only raises questions of accuracy, but also its necessity and utility.

f. Data shall Not be Kept for longer than Necessary

This is the Fifth Data Protection Principle. It was already argued above that necessity and proportionality were not satisfied for the cyclical 12-month retention period, and therefore, this Principle is also breached.

7.8 Article 6

a. Presumption of Innocence

Chapter 4 argued how and why data retention engaged Article 6(2) (presumption of innocence) with reference to *S and Marper* and the stigmatisation it can bring,[820] the RCC's assertion that data retention overturning the presumption of innocence,[821] the CJEU acknowledging data retention not distinguishing between suspects,[822] the arguments made by Milaj and Bonnici[823] and Galetta,[824] the position on substantially affected person and the ECHR being a 'living instrument.'

The main target of Article 6(2), Mendola suggests is 'avoiding a situation where such innocent persons would be subjected to explorative, criminal, investigative activities.'[825] Mendola noted that key to understanding the presumption of innocence is understanding the concept of reasonable suspicion and defining offences,[826] in which offences must be *specific and concrete*.[827] Reasonable suspicion and the nature of offences were discussed in sections 7.4(B)(2)(ii)(a) and 7.4(B)(2)(i) respectively. Both sections highlighted that data retention was neither based upon reasonable suspicion nor were offences that could justify retention were defined. Thus, in order to increase the protection of the presumption of innocence, the ECtHR would need to develop this as we enter the era of crime prediction,[828] or else we will become a

[818] ibid.
[819] Manon Oostveen, 'Identifiability and the applicability of data protection to big data' (2016) International Data Privacy Law 0:0 1, 5.
[820] *S and Marper*, (n107), [122].
[821] Romania Constitutional Court, (n148).
[822] *Digital Rights Ireland and Seitlinger and Others*, (n2), [59]; *Tele2 Sverige AB and Watson*, (n3), [106].
[823] Jonida Milaj and Jeanne Pia Mifsud Bonnici, 'Unwitting subjects of surveillance and the presumption of innocence' (2014) Computer Law and Security Review 30:4 419.
[824] Antonella Galetta, 'The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?' (2013) European Journal of Law and Technology 4:2 <http://ejlt.org/article/view/221/377> accessed 16 May 2017.
[825] Marco Mendola, 'One Step Further in the 'Surveillance Society': The Case of Predictive Policing' (2016) <http://techandlaw.net/wp-content/uploads/2016/10/One-Step-Further-in-the-Surveillance-Society_The-Case-of-Predictive-Policing.pdf> accessed 24 August 2017, p11.
[826] ibid, p12.
[827] ibid, p14.
[828] ibid, p23.

nation of suspects.[829] David Anderson's report of the investigatory powers review is titled *A Question of Trust*, yet at the same time of asking for trust, those that exercise said powers do not trust those whom they are supposed to protect.

b. Self-Incrimination

As Fischer notes, self-incrimination only applies to the active cooperation of the accused in which he notes that 'an obligation to retain and disclose home grown private traffic data as a form of forced active cooperation.'[830] This is possible under the IPA 2016 due to the definition of telecommunications operator as Chapter 6 noted. Moreover, as Smith noted and highlighted in Chapter 6, s.87(9)(b) makes it possible for telecommunications operators 'require a third party to generate and hand over communications data' to them.[831] If this third party is a user, then the self-incrimination implications become more apparent.

c. Effective Legal Assistance

The ECtHR has noted that the accused's rights to communicate with his advocate out of hearing of a third person *is part of the basic requirements of a fair trial in a democratic society* and follows from Article 6(3)(c) (author's emphasis). Section 7.6((C)(c)(v)(b)(i) discussed how data retention would impact upon legal effective assistance and the material breach of legal privilege it would cause. Any *limitation on relations between clients and lawyers, whether inherent or express*, should not thwart the effective legal assistance to which a defendant is entitled (author's emphasis).[832] Additionally, *any* interference with privileged material 'should be exceptional, be justified by a pressing need and will always be subjected to the strictest scrutiny' (author's emphasis).[833] Data retention in its current form would not only breach Article 6(3)(c), but also Article 6(1) (fair trial).[834]

7.9 Article 14 Discrimination

Chapter 4 highlighted how Article 14 ECHR was applicable to data retention under the umbrella of 'other status' and is similarly applicable to Articles 6, 8-11 and Article 2 Protocol 4. Data retention fails to discriminate between suspects and non-suspects, the legal profession and journalism etc. Indiscriminate data retention triggers what is known as *Thlimmenos* discrimination in that:

> [T]he right not to be discriminated against in the enjoyment of the rights guaranteed under the Convention is also violated when States without an objective and reasonable justification *fail to treat differently persons whose situations are significantly different* (author's emphasis).[835]

---

[829] Liberty's, 'Liberty's Submission to the Joint Committee on the Draft Communications Data Bill' (August 2012) <http://www.liberty-human-rights.org.uk/pdfs/policy12/liberty-submission-to-the-draft-communications-data-bill-committee-aug-2012-.pdf> accessed 24 August 2017.
[830] Conrad Fischer, 'Communications Network Traffic Data' (2010) <http://alexandria.tue.nl/extra2/689860.pdf> accessed 17 May 2017, p189-190.
[831] Graham Smith, (n92).
[832] *Sakhnovskiy v Russia* App no. 21272/03 (ECHR, 2 November 2010), [102].
[833] *Khodorkkovsky and Lebedev v Russia* App nos. 11082/06 and 13772/05 (ECHR, 25 July 2013), [627].
[834] ibid, [629].
[835] *Thlimmenos v Greece* App no. 34369/97 (ECHR, 6 April 2000), [44].

This would ultimately lead to a violation of all the Convention Rights mentioned above in conjunction with Article 14[836] as no objective reasonable justification could be made to support the argument of capturing massive amounts of communications data when it has been acknowledged most retained data is irrelevant.

Another Article 14 issue is the potential created by the CJEU in *Tele2 and Watson* with regards to geographical tailored data retention. The CJEU did not define 'public' (which is much lower than the ECHR threshold of reasonable suspicion)[837] or what would constitute geographical or multiple geographical areas.[838] This left Anderson wondering if the CJEU meant that it was acceptable to perform general and indiscriminate data of a particular town, or housing estate?[839] As O'Neil suggests, 'geography is a highly effective proxy for race.'[840] Although such geographical limitations may serve to limit a catch all power, this would still constitute a general and indiscriminate power based on residence,[841] which would again attract the application of Article 14.[842] Even if such a retention notice was based upon objective criteria i.e. statistics on crimes per area[843] this would not be reasonable (or proportionate, or even relevant)[844] as this too would fail to distinguish residents in a significantly different position and would lead to residential profiling. Just as the GC in *S and Marper* found a violation of Article 8 even within a confined situation, ICO regarded a surveillance measure applied to a Parish of 15781 residents[845] as incompatible with Article 8.[846] Moreover, the GC in *Zakharov* noted that Russia's surveillance measures, which amongst other things allowed 'interception of all telephone communications in *the area* where a criminal offence has been committed'[847] violated Article 8 of the ECHR.[848] This demonstrates the legal frailty of the CJEU permitting geographical data retention. This becomes all the more problematic when the CJEU did not rule on an acceptable retention time period in which under the IPA 2016 has been argued to be unnecessary and disproportionate, nor did it thoroughly critique the catalogue of human rights implications posed by data retention.

[836] ibid, [55].
[837] Matthew White, (n4), 35.
[838] ibid, 26.
[839] David Anderson, 'CJEU judgment in Watson' (21 December 2016) <https://terrorismlegislationreviewer.independent.gov.uk/cjeu-judgment-in-watson/> accessed 25 August 2017.
[840] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Penguin Books 2017), 87.
[841] Matthew White, (n4), 36.
[842] *Carson v UK* App no. 42184/05 (ECHR, 16 March 2010), [70-1].
[843] Matthew White, (n4), 26-7.
[844] As the statistics only demonstrate the propensity of crime in a given area, it does not demonstrate how and why communications data retention would be necessary and proportionate.
[845] UK Census Data for Royston <http://www.ukcensusdata.com/north-hertfordshire-e07000099> accessed 25 August 2017.
[846] ICO Enforcement Notice, (23 July 2012), (n792).
[847] *Roman Zakharov*, (n6), [265].
[848] ibid, [305].

Big Data could lead to biases based on what telecommunications are obligated to generate for law enforcement (due to ethnic profiling,[849] which can intensify ethnic profiling)[850] or inherent within the operations of the telecommunications operators.[851] Biases[852] based on race,[853] (acknowledged by the ECtHR)[854] gender and socio-economic background[855] would all fall under the ambit of Article 14. This relates to what Lyon describes surveillance as 'social sorting.' He continues that it 'classifies and categorizes relentlessly, on the basis of various – clear or occluded – criteria' and [i]t is often, but not always, accomplished by means of remote networked databases whose algorithms enable digital discrimination to take place.'[856] Such surveillance can create a chilling effect on the freedom of expression of ordinary citizens and a wide range of vulnerable groups.[857] Penney's research has suggested that women and younger people are more likely to be chilled and are less likely to take steps to defend themselves from regulatory actions and threats.[858] It has also been statistically demonstrated that Muslim-

[849] *Gillan and Quinton*, (n341); *S and Marper*, (n107), [38-40] and [124]; Bart van der Sloot, Dennis Broeders and Erik Schrijvers, *Exploring the Boundaries of Big Data* (Amsterdam University Press, Amsterdam 2016), 125; Bernard E. Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* (Chicago: University of Chicago Press 2007); Olivier De Schutter and Julie Ringelheim, 'Ethnic Profiling: A Rising Challenge for European Human Rights Law' (2008) Modern Law Review 71:3 358; Open Society Initiative, 'Equality under Pressure: The Impact of Ethnic Profiling' (2013) <https://www.opensocietyfoundations.org/sites/default/files/equality-under-pressure-the-impact-of-ethnic-profiling-netherlands-20131128_1.pdf> accessed 19 October 2017; Leanne Weber and Ben Bowling, *Stop and Search: Police Power in Global Context* (Routledge 2012); Bart Custers, Tal Zarsky and Bart Schermer, *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases (Studies in Applied Philosophy, Epistemology and Rational Ethics)* (Springer, Heidelberg 2013); Cheryl Thomas, 'Ethnicity and the Fairness of Jury Trialsin England and Wales 2006-2014' (2017) Criminal Law Review 11 860, 862.

[850] Bart van der Sloot, Dennis Broeders and Erik Schrijvers, (n849), 125; Joanne P. van der Leun and Maartje A.H. van der Woude, 'Ethnic profiling in the Netherlands? A reflection on expanding preventive powers, ethnic profiling and a changing social and political context' (2011) Policing and Society 21:4 444; Open Society Initiative, (n849).

[851] Lee Rainie and Janna Anderson, 'Code-Dependent: Pros and Cons of the Algorithm Age' (8 February 2017) <http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/02/08181534/PI_2017.02.08_Algorithms_FINAL.pdf> accessed 19 October 2017, p57; Latanya Sweeney, 'Discrimination in Online Ad Delivery' (28 January 2013) <https://arxiv.org/pdf/1301.6822.pdf> accessed 19 October 2017; Paul Bernal, (n42), 257-258; Stephen Buranyi, 'Rise of the racist robots – how AI is learning all our worst impulses' *The Guardian* (London, 8 August 2017) <https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses> accessed 19 October 2017.

[852] Cathy O'Neil, 'The era of blind faith in big data must end' (April 2017) <https://www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end#t-786714> accessed 17 October 2017.

[853] Kate Crawford and Ryan Calo, 'There is a Blind Spot in AI Research' (2016) Nature 538 311, 312; Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, 'Machine Bias' (23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 19 October 2017.

[854] *Gillan and Quinton*, (n341), [85].

[855] Solon Barocas and Andrew D. Selbst, 'Big Data's Disparate Impact' (2016) California Law Review 104 671.

[856] David Lyon, 'Surveillance as social sorting: computer codes and mobile bodies' in David Lyon (ed) *Surveillance as Social Sorting Privacy, risk, and digital discrimination* (Routledge 2003), 8.

[857] David Kaye, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (11 May 2016) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/12/PDF/G1609512.pdf?OpenElement> accessed 4 May 2017, para 57.

[858] Jonathon W. Penney, 'Internet surveillance, regulation, and chilling effects online: a comparative case study' (2017) Internet Policy Review 6:2; Jonathon W. Penney, 'Whose Speech Is Chilled by Surveillance?' *Slate* (New York City, 7 July 2017) <http://www.slate.com/articles/technology/future_tense/2017/07/women_young_people_experience_the_chilling_effects_of_surveillance_at_higher.html> accessed 17 August 2017.

American's change their behaviour due to government surveillance fears.[859] Artificial intelligence (AI), which can collect and analyse[860] large amounts of information learn through experience[861] also suffer from gender and racial bias.[862] As Christl and Spiekermann note 'as long as data and algorithms are secret, it is not possible to even notice or prove discrimination.'[863] This also demonstrates that 'other status' need not be solely relied upon in this regard as Article 14 covers amongst other things as race, colour, sex and religion.

7.10 Conclusions

This Chapter combines Chapters discussed previously in order to assess the compatibility of data retention as envisaged in the IPA 2016 with human rights guaranteed by the ECHR. Assessing Part 4's compatibility with the ECHR highlighted deficiencies within the CJEU's own rulings in *Digital Rights Ireland* and *Tele2 and Watson*. It is accepted that the CJEU did not specifically deal with any specific national implementation of data retention, but it did not use this opportunity to align itself with well-established ECtHR jurisprudence. This has been demonstrated by highlighting that data retention would not be accessible or foreseeable in terms of unfettered and arbitrary powers whether sporadically used, the nature of offences, persons liable, incidental retention, data by type and utility. This highlights how Part 4 is not in accordance with the law, something the CJEU had not dealt with. Under the examination of the ECHR, the utility of data retention was put into serious doubt in terms of its necessity and effectiveness, something which the CJEU accepted without detailed analysis or scrutiny. Moreover, the very idea of data retention as a legitimate aim was put under serious doubt, which for the CJEU, was an objective that satisfied the general interest. Furthermore, some problems with the CJEU's ruling in terms of what it would allow Member States to pursue under vague terms like the identifiable public, which falls below the threshold of reasonable suspicion identified by the case law of the ECtHR. Moreover, a pressing social need for data retention envisaged in Part 4 in terms of data retention, who can be obligated to retain, its length, and the types of data to be retained were also put under considerable scrutiny, something the CJEU could have ruled to be considered. With regards to geographical retention, this was highlighted as not being compatible with the ECHR. These deficiencies could be remedied by national courts asking the CJEU to clarify the position of the CFR where it offers less protection than the ECHR.[864]

---

[859] Dawinder S. Sidhu, (n654).
[860] Information Commissioners Office, 'Big data, artificial intelligence, machine learning and data protection' (2017) <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed 15 March 2018, p6.
[861] Giangiacomo Olivi, 'Europe: Artificial Intelligence, what can we learn from the GDPR?' (7 February 2017) <https://blogs.dlapiper.com/privacymatters/europe-artificial-intelligence-what-can-we-learn-from-the-gdpr/> accessed 15 March 2018.
[862] Aylin Caliskan, Joanna J. Bryson and Arvind Narayanan, 'Semantics derived automatically from language corpora contain human-like biases' (2017) Science 356:6334 183; Hannah Devlin, 'AI programs exhibit racial and gender biases, research reveals' *The Guardian* (London, 13 April 2017) <https://www.theguardian.com/technology/2017/apr/13/ai-programs-exhibit-racist-and-sexist-biases-research-reveals> accessed 15 March 2018; Dave Gershgorn, 'Google explains how artificial intelligence becomes biased against women and minorities' (28 August 2017) <https://qz.com/1064035/google-goog-explains-how-artificial-intelligence-becomes-biased-against-women-and-minorities/> accessed 15 March 2018.
[863] Wolfie Christl and Sarah Spiekermann, 'Networks of Control A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy' (2016) <http://crackedlabs.org/dl/Christl_Spiekermann_Networks_Of_Control.pdf> accessed 15 March 2018, p125-6.
[864] Case C-73/16 *Puškár* [2017] ECR I-253, Opinion of Advocate General Kokott, [128[5]).

Beyond the deficiencies of *Digital Rights Ireland* and *Tele2 and Watson* this Chapter highlighted the threat of data retention to freedom of expression, movement, association/assembly, religion/conscious, anonymity, relationships, data protection, presumption of innocence, self-incrimination, a fair trial and non-discrimination and how it is a social harm in various ways, and that in summary, threatens democracy. It demonstrated the threats specific professions such as journalism and the legal profession. This Chapter also demonstrated the continuous nature of data retention, in that one can never truly be free from such interference with fundamental rights.

This analysis considered the implications of how the law (due to its broad and vaguely defined terms) affects modern technologies extend beyond what the CJEU and others have considered with regards to traditional phone companies and Internet Service Providers (which on strict interpretation, is what *Digital Rights Ireland*/*Tele2* only applies to). This is done so by highlighting the God's-eye view of data retention in that it allows every aspect of an individual's life to be retained, by making one's cities, homes and themselves (using mind privacy as one example) a Panopticion through the use of smart technologies. This may, however change, given that a German judge has made a preliminary reference to the CJEU to question whether Gmail is an 'electronic communications service'[865] which would put it within the scope of *Digital Rights Ireland*/*Tele2*.

This Chapter has demonstrated that Part 4 of the IPA 2016 is not accessible, foreseeable, does not pursue a legitimate aim, does not satisfy a pressing social need, does not provide relevant and sufficient reasons for the measures, does not strike a fair balance and is not proportionate.

[865] OVG Munster, 'ECJ should clarify obligations of webmail providers' (26 February 2018) <http://www.ovg.nrw.de/behoerde/presse/pressemitteilungen/05_180226/index.php> accessed 4 April 2018.

Chapter 8: Conclusions

8.1 Summary

This thesis has sought to ask the question as to whether data retention in the words of the European Court of Human Rights (ECtHR) has undermined or even destroyed democracy on the grounds of defending it.[1] In order to assess this, Chapter 2 considered the politics behind data retention at a European Union (EU) and UK level. It highlighted that the UK was the main driver of data retention across the EU and utilised tragic events of acts of terrorism to justify said measures. However, harmonising data retention at the EU level was invalidated[2] by the Court of Justice of the European Union (CJEU) and then subsequently ruled that blanket indiscriminate data retention of all subscribers and all their data from all electronic communications services was not permissible under EU law.[3] Given the UK's pivotal role in data retention, the Investigatory Powers Act 2016 (IPA 2016), the threats posed to Article 8 of the European Convention on Human Rights (ECHR/Convention/Convention Rights), and the vote to leave the EU, it was necessary to consider data retention under the ECHR.

Chapter 3 went through the task of considering the types of communications data that could be retained via the IPA 2016. The aim of this Chapter was to highlight just how intrusive communications data can be, and this it should be regarded posing just as, if not a more serious interference with rights as the content of communications. Some examples of communications included usernames and passwords, which would compromise an individual's account. Other types included location data which could reveal sensitive personal data such as one's religion. Communications data in the form of Internet Connection Records (ICRs) and third party data would require interception to be retained, the very thing that is argued to distinguish it from content. Moreover, this Chapter revealed that many other forms e.g. mind data (and unknown types) of communications data could be retained, or generated for the purposes for of retention and went beyond what is considered traffic and location data under current EU law. Communications data can be used to build a precise profile of an individual, and this intensifies with Big Data in which said profiles (which can be discriminatory and intensify discrimination) are already ready available. Given that the ECtHR has acknowledged that given the technological advances since *Klass* the 'potential interferences with *email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely'* (author's emphasis).[4] Accepting that communications data retention poses just as serious of an interference with private life as interception is entirely possible under the ECtHR's 'living instrument' doctrine which interprets the Convention in light of present-day conditions.[5] In endorsing such a position, the ECtHR would not fall victim of its own doctrine of ensuring that Convention is practical and effective, and not theoretical and illusory.[6] The position argued now has support of the ECtHR in the recent case of *Big*

[1] *Klass v Germany* App no. 5029/71 (ECHR, 6 September 1978), [49].
[2] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECR I-238.
[3] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-970.
[4] *Szabo and Vissy v Hungary* App no. 37138/14 (ECHR, 12 January 2016), [53].
[5] *Tryer v United Kingdom* App no. 5856/72 (ECHR, 25 April 1978), [31].
[6] Alastair Mowbray, 'Creativity of the European Court of Human Rights' (2005) Human Rights Law Review 5:1 57.

Brother Watch. The consideration of privacy and Article 8 also highlighted its social value and why its protection is of fundamental importance.

Chapter 4 considered that data retention raised not only issues of Article 8, but of other Convention Rights. This Chapter first considered the most obvious right in question, Article 8, and how data retention interferes with this Convention Right in various ways. This Chapter highlighted that although Article 8 had its own instrumental and social value, its importance for the fulfilment of other rights became apparent. In the digital era, Article 8 was noted to be essential for the exercise of one's freedom of expression/association/assembly/religion/thought/conscious which are protected by Articles 9-11 ECHR. Article's 9-11 are important for democracy and Chapter 4 noted that Article 8 underpins them all, making it uniquely exceptional amongst the rest of the Convention Rights. Given that the ECtHR has a role to play in the promotion of democracy, it must ensure chilling effects are minimised, a way to do this is to look beyond privacy and data protection when issues of surveillance arise, and instead consider the issue in terms of collective freedoms and democracy, which is possible under the 'living instrument' doctrine. Chapter 4 also demonstrated the data retention raised issues of freedom of movement, protected under Article 2 Protocol 4 in that movements would be tracked and stored for vast majorities of the population, threatening the right to move without being traced. Moreover, Chapter 4 also noted that data retention potentially engages Article 6 ECHR with regards to the presumption of innocence discrimination issues, as it applied to all, whether they had committed a crime or were the subject of an investigation. Data retention also argued to engage Article 6 in that it could lead to self-incrimination through passwords or through neurotechnologies and mind data, or imposing obligations on individuals who are telecommunications operators. It was also argued that Article 6 was engaged in that it can interfere with effective legal assistance, by interfering with a lawyer's correspondence with their clients (Legal Professional Privilege, LPP). Finally, Chapter 4 noted that data retention raises issues of discrimination, which is protected under Article 14 ECHR on conjunction with Convention Rights. It does so in four ways, failing to treat those in a significantly different situation (suspect and non-suspect, or those whose communications data requires special protection i.e. lawyer) different, bias due to profiles created by Big Data, geographical data retention which would discriminate based on residency and can create a chilling effect to self-fulfilment if information disclosed enables discrimination.

Chapter 5 demonstrated that from a theoretical and legal perspective (utilising the ECHR, EU and UK law) that communications data retention is secret mass surveillance within surveillance. It did so by using Foucault's popularisation of the Panopticon in demonstrating that data retention puts one under a constant gaze through the collection of data with the ultimate aim of social control through one being unaware as to *when* they might be observed. This Panoptic glare also chills the expression of many. It also argued that data retention is Panspectric in that it relies on the subject's lack of awareness of the extent that they are under surveillance. In line with the Panopticon, this Chapter also highlighted how Governments and private corporations act in synergy by the former creating laws allowing the latter to conduct surveillance capitalism, in which the former utilises the spoils with their own surveillance. Data protection laws allows companies to create and generate data, which is then subsequently retained (surveillance within surveillance).

Chapter 6 demonstrated that from the Regulation of Investigatory Powers Act 2000 (RIPA 2000), to the Data Retention and Investigatory Powers Act 2014 (DRIPA 2014) to the IPA 2016, the obligation to retain has expanded from telephone companies and Internet Service

Providers (ISPs) to include websites, cloud based services, controllers of networks, devices, apps, software, hardware and Internet of Things (IoT) objects. This Chapter highlighted that the obligation to retain applies to essentially to anything that communicates. This Chapter also supplemented Chapter 4 in that it highlighted that the obligation to retain has implications for the family life and home aspects of Article 8 in that IoT devices will store, create and generate data about traditional home products. This Chapter also highlighted that the obligation to retain is not exclusive to the Secretary of State and Judicial Commissioner (JC), but also a variety of relevant public authorities. The Government is seeking to introduce authorisations by the Investigatory Powers Commissioner (IPC)[7] for this ability to ensure independence in the process. This however, overlooks the fact that the IPC is also the review and auditor of said authorisations.[8]

Chapter 7 assess the compatibility of data retention within Part 4 of the IPA 2016 with the ECHR. It first notes that the IPA 2016 is not even compatible with EU law, and then moves on to highlight some of the deficiencies in the CJEU's rulings in *Digital Rights Ireland* and *Tele2*. Using Article 8 as a template for other qualified Convention Rights (Articles 9-11, and Article 2 Protocol 4), it was argued that Part 4 was neither in accordance with the law or necessary in a democratic society, nor did it likely pursue a legitimate aim. This demonstrated that Part 4 was not accessible or foreseeable and permitted unfettered and arbitrary powers. The utility and necessity of the very idea of data retention was put under serious doubt. This Chapter also demonstrated Part 4 did not attain the threshold for requiring reasonable suspicion for the measure to be utilised. This Chapter also questioned whether it was established that there was a pressing social need for data retention in and of itself, those who could be obligated to retain, the length of retention and the types of data that could be retained. Chapter 7 also highlighted how data retention posed a threat to freedom of expression, movement, association/assembly, religion/conscious, anonymity, relationships, data protection, presumption of innocence, self-incrimination, a fair trial and non-discrimination and how it is a social harm in various ways, and that in summary, threatens democracy.

This thesis has reached the conclusion that data retention in the IPA 2016 undermines democracy as it violates several key Convention Rights that are the building blocks for any democratic society. The assault on privacy which acts as the foundation for freedom of expression/religion/conscious/thought/assembly/association, the hampering of the ability of journalists to act as the fourth state, the erosion of the presumption of innocence as well as threatening LLP, the discriminatory factor, the all-encompassing ability to obligate retention on anything that can communicate and whatever it can generate are all factors which support this conclusion. As the Czech Republic Constitution Court correctly acknowledges:

> Unless the individual enjoys the guarantee of controlling and checking the content and extent of information and data provided by them to be published, stored or used for other than the original purposes; unless they are provided with the possibility to recognise and assess the credibility of their potential communication partner and adapt their action accordingly, then their rights and freedoms are unavoidably restricted or even suppressed, and consequently, it is no longer possible to perceive such a society as free and democratic.[9]

[7] Regulation 3 of the draft Data Retention and Acquisition Regulations 2018 SI 2018, which inserts s.60A into the IPA 2016.
[8] See s.229(1)(b) of the IPA 2016.
[9] The Czech Republic Constitutional Court 2011/03/22 - Pl. ÚS 24/10, [30].

The question as to whether data retention in the IPA 2016 destroys democracy would depend on the Government of the day. What can be said is that when one considers the scale and depth of retention, whether it be communications data of one's browsing habits, app, phone or computer use, body tech use, neurotechnologies, household appliance use or just simply walking down the street in a Smart City, it may not destroy democracy, but it has certainly sown the seeds for its destruction. For this reason, it is argued that Part 4 of the IPA 2016 *certainly* undermines democracy because it is:

> The modern dream of the totalitarian police, with its modern techniques, is incomparably more terrible. Now the police dreams that one look at the gigantic map on the office wall should suffice at any given moment to establish who is related to whom and in what degree of intimacy.[10]

8.2 Contributions to knowledge and impact

a. Key Contributions to the discussion on Data Retention

In undertaking this analysis, this thesis has made several original contributions to knowledge, namely:

I. In understanding the social value privacy brings, it gives an insight into how privacy and Article 8 are important for the proper functioning of democracy. Thus, when one considers mass surveillance such as data retention, it highlights that the focus should not, and cannot solely be about an individual, but about society as a whole, because it affects the latter whether the former acknowledges it.

II. Continuing with the importance of Article 8 for democracy, this thesis highlighted how Article 8 underpins freedom of expression/association/assembly/religion/thought/conscious which are protected by Articles 9-11. Articles 9-11, in and of themselves are crucial democracy, and Article 8 supports each of them, hence its underpinning for democracy. It was demonstrated how communications data interferes with and chills said Convention Rights. Notable examples include having chilling effects on communications between parties, the search for, and exchange of ideas, journalists and their sources (including whistleblowers), minorities and women, political opinions, victims of violence willingness to come forward, the expression of religion and even the association or assembly of individuals or groups. This list is not exhaustive, but data retention ultimately impacts upon one's autonomous ability to act freely. Another aspect which adds to the knowledge in this particular area was considering data retention and its implications for Article 6. It demonstrated that data retention poses a serious threat to the presumption of innocence, self-incrimination, effective legal assistance and an overall fair trial. It did so by arguing that the way 'criminal charge' should be understood with regards to modern technology, needs to evolve as we move ever closer to a preventative state. In addition to this, due consideration was given to data retention in relation to Article 14, and it was highlighted it raises issues of failing to discriminate individuals who are in a substantially different situation (i.e. non-suspects, journalists, LPP) and the data itself which could be based on biases on what could be obligated to (generate) retain or what the telecommunications operators

[10] Tijmen Wisman, 'Privacy: Alive and Kicking' (2015) European Data Protection Law Review 1:1 80.

themselves generate. Whilst also acknowledging the addition of other Convention Rights affected by data retention, this thesis took a step further to consider Article 2 Protocol 4, although not applicable in UK law, it was important to highlight under the ECtHR's jurisprudence, data retention is capable of interfering with it. Adding to this point was the chilling effect on the freedom of movement when said movement is constantly logged and tracked. When one considers the variety of Convention Rights interfered with by data retention, it becomes clear that it is no longer, if it ever was, just an issue of privacy, data protection and/or freedom of expression.

III. This thesis has highlighted the far-reaching powers of the IPA 2016, in terms of *who* can be obligated to retain, and *what* can be retained. Due to the technologically neutral terms, it was identified data retention obligations not only fall upon telephone providers and ISPs, but websites, web-based services, cloud based services, controllers of networks (body, home, local, or wide), devices, apps, software, hardware and IoT objects. It highlighted that when one considers data retention, it can no longer be thought of just in terms of telephone companies or ISPs, but in terms of essentially any device that is connected to a network or can communicate. Only then it is possible to understand the far-reaching implications of the definition of telecommunications operator as it will encompass everyday objects as the IoT takes a hold. Not only will one's browsing habits, thoughts, feelings, movement and other activities on smart phones be subject to a 12-month retention period on a continuous basis, but everyday objects will also act as a Panopticon for one's home, one's city and even onself. When one considers what falls under the definition of telecommunications operator, then an insight into the types of communications data that can be retained materialises. In arguing that communications data retention is just as serious of an interference with Convention Rights as interception, it was demonstrated by examples, the types of data that would support this position e.g. passwords. Not only would telecommunications operators be obliged to retain your browsing habits, which can reveal sensitive personal data such as religion and sexual preference, but passwords and some would be obliged to retain the content that is embedded within the communications data. This thesis highlighted that there is no limit to the types of communications data that can be retained, either through its generation, or due to the vague terminology used, and as examples, Big Data and neurotechnologies which produce mind data was used. The ability to penetrate thoughts retain mind data would literally create CCTV for inside your head.[11] For this reason it was argued that communications data strikes at the substance of the right due to the severity of the interference, which would take a step further than the CJEU, but is feasible under the ECtHR's 'living instrument' doctrine. The extent at which the IPA 2016 expands upon who can be obligated to retain, and what, is not an issue that is yet fully realised in the discourse of data retention, yet we have already sleepwalked into it.

IV. This thesis has contributed to the understanding that communications data retention is a form a mass secret surveillance within surveillance. Surveillance is often understood as watching the 'focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction.'[12] However, data retention is not focussed and thus a new way of understanding surveillance had to be utilised. Data retention 'treats everyone as a suspect', 'monitors everyone' and 'puts

[11] Caspar Bowden, 'CCTV for inside your head Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation' (2001) <http://europe.rights.apc.org/eu/cctv_for_the_head.html> accessed 7 April 2018.
[12] David Lyon, *Surveillance Studies: An Overview* (Cambridge: Polity Press 2007), 14.

everyone under surveillance.'[13] In order to demonstrate communications data retention is surveillance, consideration was given to the Panopticon, Panspectron, the ECHR, EU and UK law. This analysis also uncovered that data retention is not only secret mass surveillance, but is secret mass surveillance within surveillance because much data is retained due to the data created and generated by surveillance capitalism.

V. This is the first in depth analysis of the compatibility of communications data retention with the ECHR that looks beyond Articles 8 and 10. In doing so, this thesis has meticulously highlighted how the interpretation of the ECHR questions the very idea of data retention. Many surveillance cases before the ECtHR are decided on whether interference is in accordance with the law i.e. legal basis, accessible and foreseeable. When applying these principles to data retention in Part 4 of the IPA 2016, it was highlighted that it was not accessible, and in particular, was not foreseeable. Given that Articles 9-11 and Article 2 Protocol 4 are qualified just as Article 8 is, it was demonstrated that if a measure is not in accordance with the law for the purposes of Article 8, it was not in accordance with the law for the purposes of Articles 9-11 and Article 2 Protocol 4. This position is supported by the jurisprudence of the ECtHR. This also highlighted a deficiency in the CJEU's approach to data retention in that it did not expressly endorse the ECtHR's approach to legality, thus giving Member State the potential to deviate from the Convention. Instead of ending the examination of Part 4 there, it was necessary to apply all of the ECHR tests to highlight the overall the illegality of data retention. With regards to a legitimate aim, it was also demonstrated that the type of retention envisaged in Part 4 would be difficult to justify even on an acceptable exception. It was further highlighted, due to the unique nature of each of the Convention Rights, it was impossible to use the same justification for interference e.g. data retention for national security purposes is not permissible under Article 9. This again, demonstrated a deficiency in the Charter of Fundamental Rights (CFR) in that so long as an undefined general interest was satisfied, data retention was permissible. This thesis does not just question the overall proportionality of data retention, it asks deeper questions as to whether there is a pressing social need for data retention envisaged in Part 4, whether the types of telecommunications operators obligated to retain are necessary, whether the types of communications data to retain are necessary and whether the 12-month retention period is necessary. When the components of data retention are broken down, especially in light of Chapters 3 and 6, it becomes apparent that there is no pressing social need for said measures. Questioning whether the reasons for data retention is relevant and sufficient revealed that the evidence to justify extending the obligations to retain, what to retain, and for how long were either insufficient or non-existent. This approach does not act upon the assumption based on what little anecdotes are provided because the efficiency of data retention in its current form has not been justified. Granted when the CJEU considered data retention, Part 4 had not been in mind, this thesis has argued that Part 4 goes further than data retention at an EU level, and thus the considerations for proportionality are not identical. In arguing that Part 4 strikes at the substance of the right (see Chapter 3), this could not be proportionate. This thesis also highlighted an alternative to data retention, advocated by many, data preservation, as a least restrictive measure. Due to the very questionable utility of data retention, and the lack of consideration for this more human rights friendly alternative, this also made Part 4

[13] Arianna Vedaschi and Valerio Lubello, 'Data Retention and its Implications for the Fundamental Right to Privacy' (2015) Tilburg Law Review 20 14, 16.

disproportionate. Finally, the question remained as to whether a fair balance was struck in the assessment of proportionality. There were several reasons highlighted that Part 4 was anything but for as follows:

1. Blanket indiscriminate data retention has not been permissible under the ECHR since *S and Marper*.
2. Most data retained is of innocent people.
3. It does not comply with EU law.
4. When the social value of privacy is considered, such measures are unjustified.
5. It creates social harms such as chilling effects in general and in specific contents such as LPP and journalistic sources. It erodes anonymity and makes surveillance the default. It turns one's city, home and even oneself into a Panopticon.
6. The 12-month period of retention is cyclical, and thus interference never truly stops.
7. The safeguards are insufficient.
8. The definition of 'crime' is not defined.
9. The alternative of data preservation is not utilised.
10. There will always be security issues in which large volumes of sensitive/personal data will be lost and used for nerfarious purposes. This will worsen due to the lack security of IoT objects.

VI. This thesis also used Article 8 ECHR as a guide for the interpretation of Article 8 CFR.

VII. Additionally, this thesis considered on the strong assertion that Article 6 was engaged and argued that this threatened the presumption of innocence. In order to respond to emerging technologies and as we move to the crime prediction era, it was strongly argued the ECtHR's approach needs to evolve, if not, we become a nation of suspects.[14] It was also highlighted how Part 4 made it possible for one to self-incriminate themselves, and threatens LPP.

VIII. This thesis also considers the discriminatory issues raised by data retention. This is not an issue that has been considered by the ECtHR or the CJEU in the surveillance context, and thus provides an insightful analysis of the issues raised based on data retention. It demonstrated that based on Article 14, data retention discriminated in four different ways, failing to differentiate those in a significantly different situation, the data itself that is retained or generated for retention could be biased, this can also reinforce biases and due to the CJEU's ruling, geographical discrimination. The latter point highlights that the CJEU could lead Member States to act in a manner incompatible with the ECHR. This analysis is useful for any law that permits ubiquitous surveillance as it will undoubtedly interfere with fundamental rights in an Article 14 non-compliant manner.

IX. This thesis also allows the principles and methodology established (particularly the ECHR analysis) throughout to be applied to other measures of surveillance. Measures such as the Home Office's proposed super-database which would combine various

[14] Liberty, 'Liberty's Submission to the Joint Committee on the Draft Communications Data Bill' (August 2012) <http://www.liberty-human-rights.org.uk/pdfs/policy12/liberty-submission-to-the-draft-communications-data-bill-committee-aug-2012-.pdf> accessed 8 April 2018.

databases in which the police, government bodies and businesses could access,[15] facial recognition and mobile phone extraction to name a few.

b. Impact: Adequacy

On 24 June 2016, the UK voted in a referendum, to leave the EU (Brexit). If the UK leaves as intended on 29 March 2019, it will become a third country for the purposes of data protection. The transfer of personal data to third countries is governed by Chapter V of the General Data Protection Regulation (GDPR).[16] Article 45(1) notes that transfers are only permissible if the European Commission (Commission) decides that the third country in question has an adequate level of data protection. The CJEU have ruled that third countries require 'a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order.'[17] The European Council draft negotiating guidelines with regards to Brexit holds the same position.[18]

The UK Government seeks to maintain the same position with regards to transfers as it currently does as an EU Member State.[19] In doing so, it has avowed that the UK is a 'safe destination for personal data with some of the strongest domestic data protection standards in the world.'[20] The UK Government does 'not see any reason for existing data flows from third countries to the UK to be interrupted'[21] because of its 'exceptionally high standards of data protection.'[22] However, Commission has had concerns with the current UK data protection framework.[23]

The Home Affairs Committee (HAC) highlighted several obstacles for the UK in its pursuit of being found adequate, but the most relevant for this thesis is the controversial IPA 2016.[24] The HAC specifically refers to data retention[25] where Murray and Cobbe have argued that Part 4 is

[15] Matthew White, 'Proposed police super-database breaks the law and has no legal basis – but the Home Office doesn't care' (9 October 2018) <https://theconversation.com/proposed-police-super-database-breaks-the-law-and-has-no-legal-basis-but-the-home-office-doesnt-care-104527> accessed 11 October 2018.
[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119.
[17] C-362/14 *Schrems* [2015] ECR-I 650, [96].
[18] European Council (Art.50) (23 March 2018) - Draft guidelines, at para 11.
[19] HM Government, 'The exchange and protection of personal data: A FUTURE PARTNERSHIP PAPER' (27 August 2017) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf> accessed 9 April 2018, at para 31.
[20] ibid.
[21] ibid.
[22] Theresa May, 'Prime Minister Theresa May's speech at the 2018 Munich Security Conference' (17 February 2018) <https://www.gov.uk/government/speeches/pm-speech-at-munich-security-conference-17-february-2018> accessed 9 April 2018.
[23] Chris Pounder, 'Letter to Dr Chris Pounder from the Ministry of Justice' (5 May 2011) <amberhawk.typepad.com/files/uk-deficiency-details_may-2011.pdf> accessed 9 April 2018; Chris Pounder, 'Question answered: "Why does the European Commission think the UK's Data Protection Act is a deficient implementation of Directive 95/46/EC?"' (6 February 2013) <amberhawk.typepad.com/amberhawk/2013/02/question-answered-why-does-the-european-commission-think-the-uks-data-protection-act-is-a-deficient-implementation-of.html> accessed 9 April 2018.
[24] Home Affairs Committee, *UK-EU security cooperation after Brexit (fourth report)* (2017-19 HC 635), para 94.
[25] ibid, para 97.

not compatible with EU law,[26] and will thus undermine the UK's ability to receive an adequacy decision.[27] However, the UK Government assert that data retention on the grounds of national security fall outside the scope of EU law and therefore *Digital Rights Ireland* and *Tele2* are not applicable.[28] The Investigatory Powers Tribunal (IPT) has sought guidance from the CJEU on precisely this matter.[29] Even if the UK Government's view is correct, the ECHR still applies,[30] and any divergence in the data protection context would make the UK inadequate.[31] When the Commission makes an adequacy decision, Article 45(2) dictates what it should take into account, notably:

a) the rule of law;
b) respect for fundamental rights and freedoms;
c) relevant legislation;
d) access of public authorities to personal data;
e) existence of effective independent supervisory authorities;
f) commitments to legally binding conventions.

With regards to c), this specifically concerns the IPA 2016. With regards to a), the rule of law is not respected because it has been argued that data retention is not in accordance with the law for the purposes of the ECHR. With regards to b), it has been argued that data retention violates a collection of Convention Rights. With regards to d), it was argued that the list of relevant public authorities able to access communications data either was insufficient or non-existent. With regards to e) the Commission has long since had concerns with the UK's supervisory authority, the Information Commissioner[32] and this thesis has highlighted that given the nature of the powers in Part 4, the independence of the JC does not change their ability to violate a) and b). Given that this thesis has strongly argued that data retention in the IPA 2016 violates many provisions of the ECHR, the UK its commitment to a legally binding convention with regards to f). It is therefore contended that this thesis has highlighted a significant obstacle for the UK to obtain a finding of adequacy.

The impact of this thesis and its contribution to highlighting that the UK does not have essentially equivalent data protection laws could hinder police and security operations, present non-tariff barriers to trade which could put the UK services industry at a competitive disadvantage.[33] The UK police could also lose access to intelligence and information that are

[26] Andrew D. Murray, 'Data transfers between the EU and UK post Brexit?' (2017) International Data Privacy Law 7:3 149, 156-162; Jennifer Cobbe, 'Casting the dragnet- communications data retention under the Investigatory Powers Act' (2018) Public Law 10, 15-19.
[27] Andrew D. Murray, (n26), 162.
[28] Home Affairs Committee, (n24), para 100.
[29] *Privacy International v the Secretary of State for Foreign and Commonwealth Affairs and Others* [2017] IPT/15/110/CH, [72].
[30] Matthew White, 'Guest post: Data Retention: I can't believe it's not lawful, can you? A response to Anthony Speaight QC' (2 March 2018) <https://paulbernal.wordpress.com/2018/03/02/guest-post-data-retention-i-cant-believe-its-not-lawful-can-you-a-response-to-anthony-speaight-qc/> accessed 9 April 2018.
[31] Chris Pounder, 'Why the UK is unlikely to get an adequacy determination post Brexit' (9 January 2017) <http://amberhawk.typepad.com/amberhawk/2017/01/why-the-uk-is-unlikely-to-get-an-adequacy-determination-post-brexit.html> last accessed 9 April 2018.
[32] Chris Pounder, 'Letter to Dr Chris Pounder from the Ministry of Justice', (n21); Chris Pounder, 'Question answered: "Why does the European Commission think the UK's Data Protection Act is a deficient implementation of Directive 95/46/EC?"', (n21).
[33] House of Lords European Union Committee, *Brexit: the EU data protection package (third report)* (2017-19 HL 7), para 110.

vital for law enforcement.[34] Thus, the UK's attempts at strengthening law enforcement, may well undermine it. Therefore, this thesis will not only incentivise the UK to comply with its ECHR obligations, but it also acts as a warning for the consequences to its economy and law enforcement should data retention continue as is. In order for the UK to achieve this it must:

> [E]nsure that retention notices (or more correctly defined as 'data preservation') or obligations 'must be used for a specific purpose, not as a general "fishing" exercise to bring in information' based on verifiable reasonable suspicion that is necessary and proportionate, through the least restrictive measure with a suitable notification system.[35]

c. *Impact and Importance Beyond UK law*

The importance of considering data retention under the ECHR given its binding nature on EU Member States[36] adds importance to the fact that as of September 2017, 40% of them surveyed by Privacy International are still transposing the Directive 2006/24,[37] and all are inconsistent with *Tele2*.[38] Thus not only are various Member States in violation of *Digital Rights Ireland* and *Tele2*, they are also failing under their ECHR obligations. There are also, as of writing, four cases pending before the CJEU on data retention.[39]The ECHR argument serves to supplement the CJEU's rulings using UK law as an example, but takes the argument beyond privacy, data protection and freedom of expression, and makes it one of a collection of other rights including those mentioned and democracy itself.

This analysis becomes all the more important as the ECHR can be said to be seen as 'holding the line' for States that are party to it, but not Member States of the EU (thus *Digital Rights Ireland* and *Tele2* not applying). In Russia, a new law will require ISPs and telecommunications companies to store communications data for three years.[40] The concern is that the Russian approach might inspire Eastern European non-EU legislators such as Azerbaijan, Armenia, Belarus, Georgia, Moldova and Ukraine to take a similar approach.[41] It is only Belarus that is not Members of the Council of Europe and thus not subject to the ECHR.

---

[34] ibid, para 5.
[35] Matthew White, 'Protection by Judicial Oversight, or an Oversight in Protection?' (2017) Journal of Information Rights, Policy and Practice 2:1, 41.
[36] Privacy International, 'National Data Retention Laws since the CJEU's Tele-2/Watson Judgment' (September 2017) <https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf> accessed 11 April 2018, p7.
[37] ibid, p12.
[38] ibid, p4.
[39] Case C-207/16 *Ministerio Fiscal*; Case C-623/17: Reference for a preliminary ruling from the Investigatory Powers Tribunal — London (United Kingdom) made on 31 October 2017 — *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*; Laurens Cerulus, 'Belgian court stirs up data retention controversy' (19 July 2018) <https://www.politico.eu/pro/belgian-court-stirs-up-data-retention-controversy/> (accessed 1 August 2018); FDN, 'French Surveillance To Be Scrutinized By The European Court Of Justice' (July 2018) <https://www.fdn.fr/retention-des-donnees-conseil-etat-juillet2018/#magicdomid371> accessed 1 August 2018.
[40] Di Oleg Soldatov, 'Data Retention under the 2016 "Yarovaya Law" in Russia: Disrupting the European Status Quo?' (17 March 2017) <https://www.filodiritto.com/articoli/pdf/2017/03/data-retention-under-the-2016-yarovaya-law-in-russia-disrupting-the-european-status-quo.html?_id8=3> accessed 12 April 2018, p2. This article refers to the law as Federal Law No. 375-FZ, however it is referred to as Article 13(2) of Federal Law No. 374 by the Library of Congress, see Peter Roudik, 'Russia: New Electronic Surveillance Rules' (18 July 2016) <https://www.loc.gov/law/foreign-news/article/russia-new-electronic-surveillance-rules/> accessed 12 April 2018.
[41] Di Oleg Soldatov, (n40), p3.

Considering data retention from an ECHR perspective is important as it can strengthen Eastern European states' understanding of the obligations under the Convention.[42] This thesis noted how the Romanian Constitutional Court (RCC) relied upon Article 8 and ECHR jurisprudence in finding that national data retention laws were unlawful.[43] When comparing the Western states and Romania's approach, Adrian Bannon noted that in a 'stark twist of fate, could it be that West is now going East and East is now going West.'[44] This demonstrates the importance of an ECHR perspective, whether the laws are from Eastern or Western European states.

Data retention is not just a European issue, but an international one as the UK influences surveillance laws abroad.[45] This thesis could have an impact on Australian data retention laws,[46] which would be difficult to challenge,[47] due to the fact that the ECtHR's jurisprudence 'has had a very important impact within Australia.'[48] References to the ECtHR have increased in recent years, and will continue to do so.[49] The ECHR has also guided and influenced thinking about human rights in Australia, which will also continue.[50] The ECtHR role with regards to human rights in Australia will become 'even more significant' as '[r]easoned, serious, balanced judicial opinions are a powerful weapon against injustice and arbitrary or ill-conceived deprivation of fundamental rights.'[51] The ECtHR will continue to influence Australia, and more importantly, 'many non-signatory countries' as it 'takes a leading part in, and stimulates, the trans-national conversation about human rights.'[52]

8.3 Limitations and a look to the future

a. Limitations

This thesis did not consider a particular aspect of Article 8 in surveillance cases with regards to notification. It has been argued that s.231 of the IPA 2016 regarding error reporting is not consistent with Article 8 jurisprudence on notification and raises Article 13 issues of s.231 being an effective remedy.[53]

---

[42] Ineta Ziemele, 'Conclusions' in Iulia Motoc and Ineta Ziemele (eds) *The Impact of the ECHR on Democratic Change in Central and Eastern Europe* (Cambridge University Press 2016), 499.
[43] Romania Constitutional Court DECISION no.12581 from 8 October 2009.
[44] Adrian Bannon, 'Romania retrenches on data retention' (2010) International Review of Law, Computers & Technology 24:2 145, 151.
[45] James Vincent, 'The UK Now Wields Unprecedented Surveillance Powers – Here's what it means' (29 November 2016) <https://www.theverge.com/2016/11/23/13718768/uk-surveillance-laws-explained-investigatory-powers-bill> accessed 8 January 2018.
[46] The Guardian, 'New law would force Facebook and Google to give police access to encrypted messages' *The Guardian* (London, 14 July 2017) <https://www.theguardian.com/technology/2017/jul/14/new-law-would-force-facebook-and-google-to-give-police-access-to-encrypted-messages?CMP=share_btn_tw> accessed 12 April 2018.
[47] Nicolas Suzor, Kylie Pappalardo and Natalie McIntosh, 'The passage of Australia's data retention regime: national security, human rights, and media scrutiny' (2017) Internet Policy Review 6:1 1, 12.
[48] Michael Kirby, 'Australia's Growing Debt to the European Court of Human Rights' (2008) Monash University Law Review 34:2 239, 260; Catherine Branson, 'The influence of human rights on judicial decision-making' (29 September 2009) <https://www.humanrights.gov.au/news/speeches/president-speeches-influence-human-rights-judicial-decision-making> accessed 12 April 2018.
[49] Michael Kirby, (n48), 260.
[50] ibid, 261.
[51] ibid.
[52] ibid.
[53] Matthew White, (n35), 39-41.

Article 3 Protocol 1, the right to free elections by secret ballot was not considered. This right concerns only the choice of legislature and not sporadic referendums,[54] such as Brexit.[55] Communications data can not only reveal if an individual was at the polling station on election day, but their voting behaviour can be revealed based upon websites visited which would violate the free and secret nature of elections.[56]

Fairness is an important aspect of Article 3 Protocol 1,[57] and manipulation of elections falls within the ambit of the ECtHR's considerations.[58] Ghosh and Scott note how Cambridge Analytica used sensitive personal data of Facebook users to 'manipulate American voters with targeted Facebook ads and social media campaigns.'[59] Facebook itself boasts about its influence on elections[60] which could be seen as hyperbolic, but dangerous nudging and manipulation are concrete concerns.[61] If communications data that is retained can be used to effect the outcomes of elections by manipulating or nudging just enough people to swing or tip[62] it in a particular way, this may raises issues as to its fairness. As the Council of Europe acknowledge:

> Whether Facebook and similar dominant online platforms may (deliberately or not) use their power to influence human voting or not is less the point than the fact that they – in principle – have the ability to influence elections.[63]

This lack of consideration for Article 3 Protocol 1 is seen as a limitation of this thesis because of its prime importance to the Convention system.[64] Privacy International have argued that one of the necessary responses to the Facebook/Cambridge Analytica scandal is to defend privacy

[54] *Moohan and Gillon v UK* App nos. 22962/15 23345/15 (ECHR, 13 June 2017), [40], [42].
[55] ibid, [41].
[56] Sandra Wachter, 'Privacy: Primus Inter Pares Privacy as a precondition for self-development, personal fulfilment and the free enjoyment of fundamental human rights' (2017) Oxford Internet Institute < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903514 > accessed 1 December 2017, p20.
[57] *Communist Party of Russia and Others v Russia* App no. 29400/05 (ECHR, 19 June 2012), [89].
[58] ibid, [111-122].
[59] Dipayan Ghosh and Ben Scott, 'Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You' *Time* (New York City, 19 March 2018) <http://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/> accessed 16 April 2018. For more discussion on data and democracy, see Twitter thread by Sarah Donaldson, (10 April 2018) <https://twitter.com/sarah_donaldson/status/983651700270657536> accessed 16 April 2018. For more on Facebook role in violating privacy see Twitter thread by Ashkan Soltani, (10 April 2018) <https://twitter.com/ashk4n/status/983726143650975749> accessed 16 April 2018.
[60] The Conservative Party, 'A real vote-winner' <https://www.facebook.com/business/success/conservative-party> accessed 18 April 2018.
[61] Wolfie Christl, 'Corporate Surveillance in Everyday Life' (June 2017) <http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf> accessed 1 August 2018, p5. See also Andrew Griffin, 'How Facebook Is Manipulating You to Vote' *The Independent* (London, 5 May 2016) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/uk-elections-2016-how-facebook-is-manipulating-you-to-vote-a7015196.html> accessed 16 April 2018.
[62] Council of Europe Committee of Experts, 'Study on the Human Rights Dimensions of Automated Data Processing Techniques (in particular algorithms) and possible Regulatory Implications' (6 October 2017) <https://rm.coe.int/study-hr-dimension-of-automated-data-processing-incl-algorithms/168075b94a> accessed 16 April 2018, p30.
[63] ibid.
[64] *Mathieu-Mohin and Clerfayt v Belgium* App no. 9267/81 (ECHR, 2 March 1987), [47].

as a fundamental right.[65] Using Article 8 and Article 3 Protocol 1 to supplement each other would strengthen the argument that data retention undermines democracy. This is because:

> Data that is inconspicuously amassed, harvested and stored through algorithmic technologies has been likened to the new "currency of power", as it can directly be employed for the micro-targeting of voters, possibly with decisive effects on elections.[66]

The Council of Europe have argued, this 'could jeopardise democracy itself'[67] which highlights the importance of Article 3 Protocol 1 as this constitutes the most important kind of expression, because 'it manifests the will of the people.'[68]

Another important Convention Right that was not considered is Article 2 Protocol 1, a right to education. Privacy fosters autonomous individuals, providing them with space to develop opinions and ideas which can contribute to society.[69] The very foundation of this thesis relies upon this notion as the power of writing, a production of knowledge can be seen as a form of resistance[70] to data retention. Article 2 Protocol 1 must also be interpreted in light of Articles 8-10,[71] and its aim is to safeguard pluralism in education which is essential for the preservation of a democratic society.[72] The ECHR requires some level of privacy 'in order to guarantee the free development of the personality through education' and '[o]nly if a safe, secure and private environment is ensured, people can freely develop their abilities.'[73] Tracking down ones movement across the Internet is likely to cause a chilling effect on writers[74] and decrease pluralism.[75] This again would have strengthened the human rights arguments against data retention.

Finally, from the perspective of the telecommunications operators, Article 1 Protocol 1, the right to property would also be relevant. Patrick Breyer has argued that data retention obligations would interfere with Article 1 Protocol 1 because it would allow the State to control the use of their property.[76] The only way for this to be proportionate is for telecommunications operators to be fully compensated for the costs of compliance.[77] Section 249 of the IPA 2016

---

[65] Privacy International, 'What UK politicians can, and must, do about the Cambridge Analytica/Facebook scandal' (23 March 2018) <https://ceasefiremagazine.co.uk/uk-politicians-can-must-cambridge-analytica-facebook-scandal/> accessed 16 April 2018.
[66] Council of Europe Committee of Experts, (n60), p30.
[67] ibid.
[68] Sandra Wachter, (n56), p20.
[69] Kirsty Hughes, 'The social value of privacy, the value of privacy to society and human rights discourse' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy Interdisciplinary Perspectives* (Cambridge University Press 2015), 229.
[70] James A. Tyner, 'Self and space, resistance and discipline: a Foucauldian reading of George Orwell's 1984' (2004) Social & Cultural Geography 5:1 129.
[71] *Folgerø and Others v Norway* App no. 15472/02 (ECHR, 29 June 2007), [84].
[72] ibid.
[73] Sandra Wachter, (n56), p12.
[74] PEN America, 'Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor' (12 November 2013) <https://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf> accessed 16 April 2018; Jon Penney, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) Berkeley Technology Law Journal 31:1 117 <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2104&context=btlj> accessed 5 May 2017.
[75] Sandra Wachter, (n56), p20.
[76] Patrick Breyer, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR' (2005) European Law Journal 11:3 365, 375.
[77] ibid.

does not guarantee full reimbursement and thus raises Article 1 Protocol 1 issues. This consideration could have had an important contribution beyond UK law as in Russia, a Russian telecommunications operator pointed out that complying with Russian data retention laws would deplete all their profits for the next 100 years.[78] Although the ECtHR does not consider future earnings to fall within Article 1 Protocol 1,[79] this thesis could have used that opportunity to make the case in this specific context using Russia as an example.

b. A look to the future

The issue of data retention is not yet settled, as the Court of Appeal recently did not find fault with DRIPA 2014's blanket and indiscriminate nature,[80] nor the High Court[81] (though has been critiqued in Chapter 7) and many EU Member States are planning to ignore the CJEU's rulings and expand data retention measures.[82] If any such measures are implemented, an ECHR approach undoubtedly become crucial. The UK Government has sought to comply with the CJEU adding a definition of serious crime for the purposes of Part 4 of the IPA 2016.[83] This new definition has been argued to broaden the definition that is already present in the IPA 2016,[84] beyond what the ECtHR accepted in *Kennedy*[85] and has been heavily criticised by Liberty for creating a conflicting, confusing and overbroad standard for when communications data can be retained.[86] Given that a Spanish court has made a preliminary reference to the CJEU as to whether serious crime should be solely determined by sentence or substance of the crime[87] to which Advocate General Saugmandsgaard Øe opined that access to communications data should not 'be confined to cases in which the offence concerned is of a serious nature.'[88] This would allow for further consideration and development of judge Pinto de Albuquerque concurring opinion in *Szabo*[89] that by not specifying the offences in which secret surveillance may be employed downgrades the principle of legality in a field where rigorous reading of the law is most needed and opens up abuse.

[78] Di Oleg Soldatov, (n40), p2.
[79] David Hart, 'A1P1 claims by photovoltaics get to the Court of Appeal' (4 May 2015) <https://ukhumanrightsblog.com/2015/05/04/a1p1-claims-by-photovoltaics-gets-to-the-court-of-appeal/> accessed 16 April 2018.
[80] Matthew White, 'Data Retention is still here to stay, for now…' (5 February 2018) <https://eulawanalysis.blogspot.co.uk/2018/02/data-retention-is-still-here-to-stay.html> accessed 17 April 2018.
[81] *Liberty v Secretary of State for the Home Department and Others* [2018] EWHC 975.
[82] IT-Pol, 'EU Member States plan to ignore EU Court data retention rulings' (29 November 2017) <https://edri.org/eu-member-states-plan-to-ignore-eu-court-data-retention-rulings/> accessed 17 April 2018.
[83] Regulation 21 of the draft Data Retention and Acquisition Regulations 2018 SI 2018, which inserts s.86(2A) into the IPA 2016.
[84] Neil Brown, 'The CLOUD Act: Cross-border Law Enforcement and the Internet' (8 April 2018) <https://www.scl.org/articles/10183-the-cloud-act-cross-border-law-enforcement-and-the-internet> accessed 17 April 2018.
[85] *Kennedy v UK* App no. 26839/05 (ECHR, 18 May 2018), [159].
[86] Liberty, 'Liberty's response to the Government's consultation on the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data (proposed amendments to the Investigatory Powers Act 2016 and Communications Data Code of Practice)' (18 January 2018) <https://www.libertyhumanrights.org.uk/sites/default/files/2018.01.18%20liberty%20consultation%20response%20FINAL.pdf> accessed 17 April 2018.
[87] Request for a preliminary ruling from the Audiencia provincial de Tarragona, Sección cuarta (Spain) lodged on 14 April 2016 — Ministerio Fiscal (Case C-207/16).
[88] Case C-207/16 *Ministerio Fiscal* [2018] ECR-I 300, Opinion of Saugmandsgaard Øe, [122].
[89] *Szabo*, (n4), Concurring Opinion of Judge Pinto de Albuquerque, [17].

The recent ECtHR Chamber judgment of *Centrum För Rättvisa v Sweden*[90] has very important implications for data retention as it was held that:

> Having regard to the present-day threats being posed by global terrorism and serious cross-border crime as well as the increased sophistication of communications technology, the decision to set up a bulk interception regime in order to identify such threats was one which fell within the respondent State's margin of appreciation.

This position has been reaffirmed in *Big Brother Watch* in which the ECtHR acknowledged that bulk interception *in principle* falls within a State's margin of appreciation.[91]This will seriously need to be considered in future works as it appears to be the first retreat of the ECtHR with regards to mass surveillance post-Snowden, inconsistent with *Zakharov* and *Szabo* and could be used as a basis to justify data retention which this thesis has argued to violate the ECHR. Future work must also consider the Home Office's plans, beyond the definition of serious crime with regards to data retention.[92] It is all the more concerning considering the Mi5/6 and GCHQ have admitted to unlawfully spying on Privacy International.[93] The acceptance of bulk interception by the ECtHR exasperates the already high inherent risk of abuse. The ECtHR has in the past unwittingly permitted the UK to conduct mass surveillance,[94] however, given the Snowden revelations and the increase in the UK's surveillance apparatus since, it is a major concern that the ECtHR is heading in the direction of the acceptance of mass surveillance.

Finally, even if one were to consider the CJEU's approach to data retention, and even this thesis which adds to the strength a victory, it may be largely symbolic 'as metadata lives a long life in the private sector' as much data will be available, 'even without a mandatory data retention scheme.'[95] This is where a greater focus on surveillance capitalism becomes key because the question becomes whether the communications data should be generated in the first place? As van der Sloot notes 'states are held, among others, to ensure adequate protection of privacy in horizontal relationships.'[96] Thus future research could consider whether the ECtHR's 'living instrument' could be utilised to supplement data protection laws by putting states under a

---

[90] *Centrum För Rättvisa v Sweden* App no. (ECHR, 19 June 2018), [179].
[91] *Big Brother Watch v UK* App nos. 58170/13, 62322/14 and 24960/15 (ECHR, 13 September 2018), [317].
[92] Home Office, 'Investigatory Powers Act 2016: Response to Home Office Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data' (June 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/724142/June_2018_IPA_regulations_-_Government_Response_to_consultation_on_response_to_ECJ_judgment.pdf> accessed 1 August 2018.
[93] Privacy International, 'Press release: UK intelligence agency admits unlawfully spying on Privacy International' (25 September 2018) <https://privacyinternational.org/press-release/2283/press-release-uk-intelligence-agency-admits-unlawfully-spying-privacy> accessed 11 October 2018; *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others* [2018] IPT/15/110/CH; 'Mi5 Report to the IPT on searches for the BPD/BCD case' <https://privacyinternational.org/sites/default/files/2018-09/8.%20MI5%20OPEN%20report%20on%20searches.pdf> accessed 11 October 2018.
[94] Matthew White, 'Guest post: Data Retention: I can't believe it's not lawful, can you? A response to Anthony Speaight QC' (2 March 2018) <https://paulbernal.wordpress.com/2018/03/02/guest-post-data-retention-i-cant-believe-its-not-lawful-can-you-a-response-to-anthony-speaight-qc/> accessed 11 October 2018.
[95] Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) European Law Review 6 835, 849.
[96] Bart van der Sloot, 'Privacy as human flourishing Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?' (2014) Journal of Intellectual Property, Information Technology and E-Commerce Law 230, 232, para 12.

positive obligation to prevent mass data generation and collection by corporations and third parties.

Bibliography

-- 'Mi5 Report to the IPT on searches for the BPD/BCD case' <https://privacyinternational.org/sites/default/files/2018-09/8.%20MI5%20OPEN%20report%20on%20searches.pdf> accessed 11 October 2018.

-- 'New law would force Facebook and Google to give police access to encrypted messages' *The Guardian* (London, 14 July 2017) <https://www.theguardian.com/technology/2017/jul/14/new-law-would-force-facebook-and-google-to-give-police-access-to-encrypted-messages?CMP=share_btn_tw> accessed 3 January 2018.

-- *Der Spiegel* (Hamburg) <http://www.spiegel.de/media/media-34103.pdf> accessed 5 January 2018.

-- Draft Council Resolution on the Interception of Telecommunications, 10090/93 (16 November 1993) <http://database.statewatch.org/e-library/1994-jha-k4-03-06.pdf> accessed 23 May 2017.

-- <http://www.iknowwhereyourcatlives.com/> accessed 14 April 2017.

-- Exchangeable image file format for digital still cameras: Exif Version 2.31, (2016) <http://www.cipa.jp/std/documents/e/DC-008-Translation-2016-E.pdf> accessed 14 April 2017.

-- The right to privacy in the digital age, Report of the Office of the High Commissioner for Human Rights, (2014) <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf accessed 24 April 201.

-- Resolution 68/167 adopted by the General Assembly on 18 December 2013, 'The right to privacy in the digital age' (21 January 2014) <http://undocs.org/A/RES/68/167> accessed 25 April 2017.

-- Resolution 2045 (2015), <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/resol_mass_surveillance_/resol_mass_surveillance_en.pdf> accessed 8 May 2017.

-- Skype for Business Team, 'Introducing free Skype Meetings' (5 July 2016) <https://blogs.office.com/2016/07/05/introducing-free-skype-meetings/> accessed 10 May 2017.

-- Rules of Court (14 November 2016) <http://www.echr.coe.int/Documents/Rules_Court_ENG.pdf> accessed 11 November 2017.

-- Hearing (7 November 2017) <https://www.echr.coe.int/Pages/home.aspx?p=hearings&w=5817013_07112017&language=en&c=&py=2017> accessed 7 June 2018.

-- A report on the Surveillance Society for the Information Commissioner (September 2006) <https://www.york.ac.uk/res/e-society/documents/20061106surveillance.pdf> accessed 22 November 2015.

-- Glossary <https://edps.europa.eu/data-protection/data-protection/glossary/a_en> accessed 30 November 2017.

-- Implement Basic Networks and Security <http://www.sqa.org.uk/e-learning/HardOSEss04CD/page_10.htm> accessed 30 November 2017.

-- Federal Networking Council Resolution, 'Definition of the 'Internet,' (24 October 1995) <https://www.nitrd.gov/fnc/Internet_res.aspx> accessed 30 November 2017.

-- Ofcom General Conditions Guidance <http://stakeholders.ofcom.org.uk/telecoms/ga-scheme/general-conditions/general-conditions-guidelines/> accessed 1 December 2017.

-- New EC Regulatory Framework for the regulation of electronic communications, <http://www.ofcom.org.uk/static/archive/oftel/ind_info/eu_directives/> accessed 20/08/2014.

-- Investigatory Powers Bill Research Group, <https://docs.google.com/document/d/1ZiEQJaBjUjc332dQnJkm1m4EOJNnoEtHN7hw5q9kHVk/edit?pref=2&pli=1> accessed 4 December 2017.
-- Actuate, <https://en.oxforddictionaries.com/definition/actuate> accessed 11 December 2017.

-- Chrome Help, 'Sync and view tabs and history across devices' <https://support.google.com/chrome/answer/2591582?hl=en-GB> accessed 5 December 2017.

-- 'What is wireless personal area networks?' <http://www.webopedia.com/TERM/W/wireless_personal_area_network.html> accessed 1 December 2015.

-- Bluetooth Technology Basics, <http://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics> accessed 6 December 2017.

-- Bluetooth devices, <http://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-devices> accessed 6 December 2017.

-- 'Results of the 2016 Global Privacy Enforcement Network Sweep' (22 September 2016) <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/bg_160922/>accessed 22 September 2016.

-- Communications Data: Draft Code of Practice – Home Office, 1 March 2016.

-- Sentencing remarks of Mr Justice Jeremy Baker in *R v Khawaja, Bhatti and Ali* at Woolwich Crown Court, 6 February 2015 <https://www.judiciary.gov.uk/wpcontent/uploads/2015/02/khawaja-sentencing-remarks1.pdf> accessed 31 July 2017.

-- 'The thing to be proved is used as one of your assumptions.' A List Of Fallacious Arguments <http://www.don-lindsay-archive.org/skeptic/arguments.html> accessed 31 July 2017.

-- UK Census Data for Royston <http://www.ukcensusdata.com/north-hertfordshire-e07000099> accessed 25 August 2017.

2013 Annual Report of the Interception of Communications Commissioner (HC 1184 8 April 2014).

Abelson H, Anderson R, Bellovin S.M, Benaloh J, Blaze M, Diffie W, Gilmore J, Green M, Landau S, Neumann Peter.G, Rivest R.L, Schiller J.I, Schneier B, Specter M and Weitzner Daniel.J, 'Keys under doormats: mandating insecurity by requiring government access to all data and communications' (2015) Journal of Cybersecurity 1.

Acar G, Englehardt S, and Narayanan A, 'No boundaries for user identities: Web trackers exploit browser login managers' (27 December 2017) <https://freedom-to-tinker.com/2017/12/27/no-boundaries-for-user-identities-web-trackers-exploit-browser-login-managers/> accessed 2 January 2018.

Adegoke, Y, 'Eurotel to launch virtual ISP services' (2003) New Media Age 1, 9.

Agarwal A, 'Access your Passwords from Anywhere with Google Password Manager' (1 February 2016) <https://www.labnol.org/internet/google-passwords-manager/29077/> accessed 10 April 2017.

Ahmed K, 'Secret plan to spy on all British phone calls' *The Guardian* (London, 3 December 2003) <https://www.theguardian.com/uk/2000/dec/03/kamalahmed.theobserver> accessed 26 May 2017.

All Party Parliamentary Internet Group, 'Communications Data: Report of an Inquiry by the All Party Internet Group' (January 2003) <https://www.cl.cam.ac.uk/~rnc1/APIG-report-commsdata.pdf> accessed 12 August 2017.

Almehmadi A, *The Spy in Your Pocket* (CreateSpace Independent Publishing Platform 2017).

Anderson D, 'A Question of Trust, Report of the Investigatory Powers Review' (June 2015, <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf> accessed 2 March 2016.

-- 'Davis/Watson appeal' (20 November 2015) <https://terrorismlegislationreviewer.independent.gov.uk/daviswatson-appeal/> accessed 18 June 2017.

-- 'Report of the Bulk Powers Review' (August 2016) <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf> accessed 2 November 2016.

-- ‘CJEU judgment in Watson’ (21 December 2016) <https://terrorismlegislationreviewer.independent.gov.uk/cjeu-judgment-in-watson/> accessed 25 August 2017.

Andrejevic M, ‘The work of watching one another: Lateral surveillance, risk, and governance’ (2005) Surveillance & Society 2:4 479.

-- *iSpy: Surveillance and power in the interactive era* (Lawrence, KA: University Press of Kansas 2007).

-- ‘Privacy, exploitation, and the digital enclosure’ (2009) Amsterdam Law Forum 1:4 47.

-- *Infoglut: How Too Much Information is Changing the Way We Think and Know* (Routledge 2013).

-- ‘The Big Data Divide’ (2014) IJoC 8 1673.

-- Operational Case for the Retention of Internet Connection Records < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473769/Internet_Connection_Records_Evidence_Base.pdf> accessed 7 August 2017.

-- ‘Redegørelse om diverse spørgsmål vedrørende logningsreglerne’ (December 2012) <http://www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf> accessed 10 August 2017.

Angwin J, Larson J, Mattu S and Kirchner L, ‘Machine Bias’ *ProPublica* (Ney Work City, 23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 19 October 2017.

Annual Report of the Chief Surveillance Commissioner, HC 498 SG/2012/127.

Apple, ‘Apple Introduces “Jaguar,” the Next Major Release of Mac OS X’ (17 July 2002) <http://www.apple.com/pr/library/2002/07/17Apple-Introduces-Jaguar-the-Next-Major-Release-of-Mac-OS-X.html > accessed 6 December 2017.

Apthorpe N, Reisman D, Sundaresan S, Narayanan A and Feamster N, ‘Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic’ (2017) <https://arxiv.org/pdf/1708.05044.pdf> accessed 8 December 2017.

Apthorpe N, Reisman D and Feamster N, ‘A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic’ (2016) <https://arxiv.org/pdf/1705.06805.pdf> accessed 8 December 2017

Arato, ‘Constitutional Transformation in the ECtHR: Strasbourg's Expansive Recourse to External Rules of International Law’ (2012) Brooklyn Journal of International Law 37:2.

A Report by DATA-PSST and DCSS, ‘Public Feeling on Privacy, Security and Surveillance’ (November 2015) <https://sites.cardiff.ac.uk/dcssproject/files/2015/11/Public-Feeling-on-Privacy-Security-Surveillance-DATAPSST-DCSS-Nov2015.pdf> accessed 13 January 2017.

A review by InTechnology of legislation and regulation concerning data storage in the UK and Europe <http://www.arrowecs.co.uk/dns_cms/uploadedfiles/dns/managed_services/inpartnership/making_sense_of_data_law.pdf> accessed 7 August 2017.

Arnardóttir O.M, 'The Differences that Make a Difference: Recent Developments on the Discrimination Grounds and the Margin of Appreciation under Article 14 of the European Convention on Human Rights' (2014) HRLR 14:4 647.

Article 29 Working Party, 'Opinion 4/2001 On the Council of Europe's Draft Convention on Cyber-crime' <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp41_en.pdf> accessed 13 August 2017.

-- 'Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)]' (9 November 2004) < http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp99_en.pdf> accessed 12 August 2017.

-- 'European Data Protection Authorities find current implementation of data retention directive unlawful' (14 July 2010) <http://ec.europa.eu/justice/policies/privacy/news/docs/pr_14_07_10_en.pdf> accessed 5 June 2017.

-- Opinion 03/2013 on purpose limitation' (2 April 2013) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 22 August 2017.

-- 'Advice paper on special categories of data ("sensitive data")' (4 April 2011) <http://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf> accessed 22 August 2017.

-- 'Opinion 13/2011 on Geolocation services on smart mobile devices' (adopted 16 may 2011) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf> accessed 13 April 2017.

-- 'Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector' (27 February 2014) < http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf> accessed 22 August 2017.

-- 'Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)' (July 2016) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf> accessed 21 October 2016.

-- Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC).

-- letter to Microsoft (12 January 2016) <http://ec.europa.eu/newsroom/document.cfm?doc_id=42572> accessed 24 April 2017.

-- letter to Microsoft (15 February 2017) <http://ec.europa.eu/newsroom/document.cfm?doc_id=42947> accessed 24 April 2017.

-- 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (9 April 2014) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 23 November 2017.

Ashbrook D and Starner T, 'Using GPS to learn significant locations and predict movement across multiple users' (2003) Pers. Ubiquitous Comput. 7:5 275.

Aston V, 'State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives' (2017) EJLT 8:1 <http://ejlt.org/article/view/548/730> accessed 28 April 2017.

Atzori L, Iera A and Morabito G, 'The Internet of Things: A survey' (2010) Computer Networks 54:15 2787.

Aviram A, 'Revealed: Bristol's police and mass mobile phone surveillance' (October 2016) <https://thebristolcable.org/2016/10/imsi/> accessed 22 October 2016.

Backstrom L, Sun E and Marlow C, 'Find Me If You Can: Improving Geographical Prediction with Social and Spatial Proximity' (2008) <http://cameronmarlow.com/media/backstrom-geographical-prediction_0.pdf> accessed 14 April 2017.

Babuta A, 'Big Data and Policing An Assessment of Law Enforcement Requirements, Expectations and Priorities' (September 2017) <https://rusi.org/sites/default/files/201709_rusi_big_data_and_policing_babuta_web.pdf> accessed 19 October 2017.

Baines J, 'Don't be so soft' (22 November 2016) <https://informationrightsandwrongs.com/2016/11/22/dont-be-so-soft/> accessed 23 November 2016.

Baker A, 'The Enjoyment of Rights and Freedoms: A New Conception of the 'Ambit' under Article 14 ECHR' (2006) MLR 69:5 714.

Balkan A, 'The nature of the self in the digital age' (3 March 2016) <https://ar.al/notes/the-nature-of-the-self-in-the-digital-age/> accessed 13 November 2017.

Ball N, 'Security versus Privacy: A De-Actualizing Formulation' (28 January 2015), <http://www.globalresearch.ca/security-versus-privacy-a-de-actualizing-formulation/5427499> accessed 7 March 2017.

Bamford J, 'The Most Wanted Man in the World' *Wired* (San Francisco, California, 13 June 2014) <http://www.wired.com/2014/08/edward-snowden/> accessed 10 April 2017.

Banks T, 'MAC and IP Addresses: Personal Information?' (24 July 2012) <http://www.privacyanddatasecuritylaw.com/mac-and-ip-addresses-personal-information> accessed 10 April 2017.

Bannon A, 'Romania retrenches on data retention' (2010) International Review of Law, Computers & Technology 24:2 145.

Barabas E, 'European Court of Justice: EU Data Retention Directive Infringes on Human Rights' (April 10 2014) <https://cdt.org/blog/european-court-of-justice-eu-data-retention-directive-infringes-on-human-rights/> accessed 12 June 2017.

Barclay C, House of Commons Library Research Paper 00/25 'The Regulation of Investigatory Powers Act' (March 2000) <http://researchbriefings.files.parliament.uk/documents/RP00-25/RP00-25.pdf> accessed 30 November 2017.

Barfield W and Williams A, 'Law, Cyborgs, and Technologically Enhanced Brains' (2017) Philosophies 2:6.

Barnett M and Duvall R, 'Power in International Politics' (2005) International Organization, 59:1 39

Barocas S and Selbst A.D, 'Big Data's Disparate Impact' (2016) California Law Review 104 671.

Bates E, *The Evolution of the European Convention on Human Rights: From Its Inception to the Creation of a Permanent Court of Human Rights* (Oxford University Press, 2010).

BBC, 'Safeguard over e-mail 'snooping' Bill' *BBC News* (London, 13 July 2000) <http://news.bbc.co.uk/1/hi/uk/830968.stm> accessed 15 November 2017.

-- 'Previous cases of missing data' *BBC News* (London, 25 May 2009) <http://news.bbc.co.uk/1/hi/uk/7449927.stm> accessed 10 October 2017.

-- 'Theresa May says 'lives at risk' without data surveillance' *BBC News* (London, 15 January 2015) <http://www.bbc.co.uk/news/uk-politics-30816331> accessed 20 November 2016.

Belgium's Draft Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions (2002) <http://www.statewatch.org/news/2002/aug/05datafd.htm> accessed 25 May 2017.

Bentham J, The Works of Jeremy Bentham, vol. 4 [1843] (September 2011) <http://lf-oll.s3.amazonaws.com/titles/1925/Bentham_0872-04_EBk_v6.0.pdf> accessed 3 November 2016

Bentham M, 'Police 'must be given power to shut websites in child abuse and revenge porn fight'' *The Standard* (16 December 2016) <http://www.standard.co.uk/news/crime/police-

must-be-given-power-to-shut-websites-in-child-abuse-and-revenge-porn-fight-a3422131.html> accessed 17 July 2017.

Bernal P, 'Terrorism and knee-jerk legislation…' (23 May 2013) <https://paulbernal.wordpress.com/2013/05/23/terrorism-and-knee-jerk-legislation/> accessed 29 May 2017.

-- *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge Intellectual Property and Information Law 2014).

-- 'Data gathering, surveillance and human rights: recasting the debate,' (2016) Journal of Cyber Policy 1:2 243.

-- 'A few words on 'Internet Connection Records'' (5 November 2015) <https://paulbernal.wordpress.com/2015/11/05/a-few-words-on-internet-connection-records/> accessed 5 April 2017.

Berner M, Graupner E and Maedche A, 'The Information Panopticon in the Big Data Era' (2014) Journal of Organization Design 3:1 14.

Biermann K, 'Betrayed by our own data' (10 March 2011) <http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz> accessed 13 April 2017.

Big Brother Watch, 'Briefing Note: Why Communications Data (Metadata) Matter' (July 2014) <https://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/07/Communications-Data-Briefing.pdf> accessed 9 October 2017.

-- 'Internet Connection Records' (March 2016) <https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Internet-Connection-Records.pdf> accessed 10 October 2017.

Bignami F.E, 'Privacy and Law Enforcement in the European Union: the Data Retention Directive' (2007) Chicago Journal of International Law 8 233.

Bingham Centre for the Rule of Law, 'Meeting Report: EU Law, the Investigatory Powers Act, and UK-EU Cross-Border Crime and Security Cooperation' (17 March 2017) <https://www.biicl.org/documents/1634_2017-04-29_-_appg_report_14_march_2017.pdf?showdocument=1> accessed 22 June 2017.

Bjorge E, 'National supreme courts and the development of ECHR rights' (2011) Int J Const Law 9:1 5.

Biselli A, 'EU discusses future of data retention: "Indiscriminate retention no longer possible"' (31 May 2017) <https://edri.org/eu-discusses-future-of-data-retention-indiscriminate-retention-no-longer-possible/> accessed 22 June 2017.

Bisson D, Mass-surveillance 'undermines security' and failed to stop 9/11 attacks, says ex-NSA officer, (6 January 2016), <https://www.grahamcluley.com/mass-spying-undermines-security-failed-stop-911-attacks-says-nsa-officer/> accessed 8 March 2017.

BITDEFENDER, 'The hidden risks of bringing the Internet of Things into your home' (10 December 2015) <http://mashable.com/2015/12/10/iot-home-security-brandspeak/#z4F6Xk4zrsqF> accessed 8 December 2017.

Blanchette F and Johnson D.G, 'Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness' (2002) The Information Society 18 33.

Blumberg A.J and Eckersley P, 'On Locational Privacy, and How to Avoid Losing it Forever' (August 2009) <https://www.eff.org/files/eff-locational-privacy.pdf> accessed 13 May 2017.

Blumenstock J, Cadamuro G and On R, 'Predicting poverty and wealth from mobile phone metadata' (2015) Science 350:6264 1073.

Boehm and Paul de Hert, *The rights of notification after surveillance is over: ready for recognition?* (Yearbook of the Digital Enlightenment Forum, IOS Press 2012).

Boehm F and Mark D. Cole, 'Data Retention after the Judgement of the Court of Justice of the European Union' (30 June 2014) <http://www.zar.kit.edu/DATA/veroeffentlichungen/237_237_Boehm_Cole-Data_Retention_Study-June_2014_1a1c2f6_9906a8c.pdf> accessed 31 May 2018

Bogard W, 'Surveillance assemblage and lines of flight' in David Lyon (ed) Online monitoring, filtering, blocking Online monitoring, filtering, blocking *Theorizing surveillance: The Panopticon and Beyond* (Portland, OR: Willan 2006).

Boiten and Julio Hernandez-Castro, 'Can you really be identified on Tor or is that just what the cops want you to believe?'*The Conversation* (Melbourne, 25 July 2014), <https://theconversation.com/can-you-really-be-identified-on-tor-or-is-that-just-what-the-cops-want-you-to-believe-29430> accessed 30 July 2017.

Bond R.M. Fariss C.J, Jones J.J, Kramer A.D.I, Marlow C, Settle J.E and Fowler J.H, 'A 61-million-person experiment in social influence and political mobilization' (2012) Nature 489 295.

Booth R, 'Three UK's mobile customers experience new data breach' *The Guardian* (London, 20 March 2017) <https://www.theguardian.com/business/2017/mar/20/three-mobile-possible-data-breach-data-usage-call-history> accessed 21 August 2017.

Botero C, Inter-American Commission on Human Rights, 'Freedom of Expression on the Internet' (2013) <https://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf> accessed 1 May 2017.

Bowcott O, 'EU's highest court delivers blow to UK snooper's charter' *The Guardian* (London, 21 December 2016) <https://www.theguardian.com/law/2016/dec/21/eus-highest-court-delivers-blow-to-uk-snoopers-charter> accessed 21 June 2017.

Bowden C, 'CCTV for inside your head Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation' (2001) <http://europe.rights.apc.org/eu/cctv_for_the_head.html> accessed 23 May 2017.

-- 'Closed circuit television for inside your head: blanket traffic data retention and the emergency anti-terrorism legislation' (2002) Duke Law and Technology Review 1 1.

-- 'Digital Surveillance, Chapter Five Part I' (28 April 2013) <https://www.openrightsgroup.org/ourwork/reports/digital-surveillance/chapter-five-part-I> accessed 25 May 2017.

-- 'Privacy and Security Inquiry: Submission to the Intelligence And Security Committee of Parliament' (7 February 2014) <https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/public-evidence/12march2015/20150312-P%2BS-043-Bowden.pdf?attachauth=ANoY7cqU8inv9fTxZ5MVi5GPhH0Z2u9gkKE7yMB3iOOO89VdSiEN3jI_Ak_xqpbYL1eQHrmbf5djj_q8ZnEpOgM8X-oweDJFf2RmI0I-O9mSIsTDPblG9aNZbdSghnH3hjSFNeyj0idMFJxlPGsqFwiOJiQfItgKrRlkNim0nEl2X5UoLhXHm-05_0t75ZdO06d_S6o1OB_dfabXLGl1xCuUmgiwRsOKcn81egRMDl8CfDIO0EedX3OjJPuD7X2uVYQqYeC8u_ddz3neWhhIzB-70lTFQLBlcw%3D%3D&attredirects=0> accessed 4 January 2018.

boyd d and Crawford K, 'Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon' (2012) Information, Communication & Society 15 665.

Boyle J, 'Foucault in cyberspace' (1997) University of Cincinnati Law Review 66:1 177.

Braman S, 'Tactical memory: The politics of openness in the construction of memory' (2006) First Monday 11:7.

Branson C, 'The influence of human rights on judicial decision-making' (29 September 2009) <https://www.humanrights.gov.au/news/speeches/president-speeches-influence-human-rights-judicial-decision-making> accessed 12 April 2018.

Brayne S, 'Big Data Surveillance: The Case of Policing' (2017) American Sociology Review 82:5 977.

Brems E, 'Human Rights: Minimum and Maximum Perspectives' (2009) HRLR 9:3 349.

Brems E and Lavrysen L, ''Don't Use a Sledgehammer to Crack a Nut': Less Restrictive Means in the Case Law of the European Court of Human Rights' (2015) HRLR 15:1 139.

Brdar S, Ćulibrk D, Crnojević V, 'Demographic Attributes Prediction on the Real-World Mobile Data' (June 2012) <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.296.1374&rep=rep1&type=pdf> accessed 14 April 2017.

Breyer P, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR' (2005) European Law Journal 11:3 365.

Breyer v Germany App no. 50001/12 Communicated on 21 March 2016; Written submissions (5 September 2016) <https://www.article19.org/data/files/medialibrary/38485/Breyer-v-Germany---App.-No.-50001-12.pdf> accessed 29 April 2017.

Brooke H, 'Mass surveillance: my part in the reform of GCHQ and UK intelligence gathering' *The Guardian* (London, 14 July 2015) <https://www.theguardian.com/commentisfree/2015/jul/14/mass-suveillance-reform-gchq-uk-intelligence-gathering-rusi-report> accessed 2 November 2016.

Brown I, 'Communications Data Retention in an Evolving Internet' (2010) International Journal of Law and Information Technology 19:2 95.

Brown K.V, 'Here Are the First Hints of How Facebook Plans to Read Your Thoughts' *Gizmodo* (21 September 2017) <https://gizmodo.com/here-are-the-first-hints-of-how-facebook-plans-to-read-1818624773> accessed 9 November 2017.

Brown N, 'An assessment of the proportionality of regulation of 'over the top' communications services under Europe's common regulatory framework for electronic communications networks and services' (2014) Computer Law & Security Review 30:4 357.

-- 'A Quick Overview of the Draft Investigatory Powers Bill' (4 November 2015) <http://www.scl.org/site.aspx?i=ed44789> accessed 4 December 2017.

-- 'The CLOUD Act: Cross-border Law Enforcement and the Internet' (8 April 2018) <https://www.scl.org/articles/10183-the-cloud-act-cross-border-law-enforcement-and-the-internet> accessed 17 April 2018.

Bruno G and Nolter C, 'Millions of Time Warner Cable Customers' Information Exposed' (1 September 2017) <https://www.thestreet.com/story/14291954/1/millions-of-time-warner-cable-customer-s-information-exposed-after-data-leak.html> accessed 8 September 2017.

BT Broadband Privacy Policy <https://www.productsandservices.bt.com/products/static/privacy-policy/?page=Broadband> accessed 17 April 2017.

Bublitz J-C, 'My Mind Is Mine!? Cognitive Liberty as a Legal Concept' in Elisabeth Hildt and Andreas G. Franke (ed), *Cognitive Enhancement An Interdisciplinary Perspective* (Dordrecht: Springer 2013).

Bucholski M, 'Surveillance and sousveillance on Facebook: Between empowerment and disempowerment' (2016) MaRBLE Research Papers Vol III, 22.

Bulak B and Zysset A, '"Personal Autonomy" and "Democratic Society" at the European Court of Human Rights: Friends or Foes?' (2013) UCL Journal of Law and Jurisprudence 2 <http://discovery.ucl.ac.uk/1470685/1/2UCLJLJ230%20-%20Personal%20Autonomy.pdf> accessed 8 May 2017.

Bundesverfassungsgericht, 'Data retention unconstitutional in its present form' (March 2010) <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html > accessed 4 April 2017.

Buranyi S, 'Rise of the racist robots – how AI is learning all our worst impulses' *The Guardian* (London, 8 August 2017) <https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses> accessed 19 October 2017.

Burbergs M, 'How the right to respect for private and family life, home and correspondence became the nursery in which new rights are born: Article 8 ECHR' in Eva Breams and Janneke Gerards (eds) *Shaping Rights in the ECHR: The Role of the European Court of Human Rights in Determining the Scope of Human Rights* (Cambridge University Press).

Cadwalladr C, 'Google, democracy and the truth about internet search' *The Guardian* (London, 4 December 2016, <https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook?CMP=share_btn_tw> accessed 9 December 2016.

Caliskan A, Bryson J.J and Narayanan A, 'Semantics derived automatically from language corpora contain human-like biases' (2017) Science 356:6334 183.

Campbell D, 'Intercepting the Internet' *The Guardian* (London, 29 April 1999) <https://www.theguardian.com/technology/1999/apr/29/onlinesupplement3> accessed 31 May 2018.

Cannataci J.A, 'Report of the Special Rapporteur on the right to privacy' (24 February 2017) A/HRC/34/60.

Cappato M,'European Parliament, 2nd Report on the proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector' (24 October 2001) <http://www.statewatch.org/news/2001/nov/cappato.pdf> accessed 23 May 2017.

Carrefax, 'Twitter Joke Trial | WLR (D) Case Summary' (1 August 2012) <https://carrefax.wordpress.com/2012/08/01/twitter-joke-trial-wlr-d-case-summary/> accessed 1 December 2017.

Castells M, *The power of identity* (Malden, MA: Blackwell 2004).

Cellan-Jones R, 'Web surveillance - who's got your data?' *BBC News* (London, 2 April 2002) <http://www.bbc.co.uk/news/technology-17586605> accessed 4 December 2017.

Center for Democracy and Technology, '"Regardless of Frontiers" The International Right to Freedom of Expression in the Digital Age' (April 2011) <https://cdt.org/files/pdfs/CDT-Regardless_of_Frontiers_v0.5.pdf> accessed 6 May 2017.

Centre for Strategy and Evaluation Services, 'Evidence of Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries' (2012) <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-

do/policies/police-cooperation/data-retention/docs/drd_task_2_report_final_en.pdf> accessed 13 August 2017.

Cerulus L, 'Belgian court stirs up data retention controversy' (19 July 2018) <https://www.politico.eu/pro/belgian-court-stirs-up-data-retention-controversy/> (accessed 1 August 2018).

Chapple M, 'Wireshark tutorial: How to sniff network traffic' *TechTarget* (Newton, Massachusetts, October 2008) <http://searchsecurity.techtarget.com/tip/Wireshark-tutorial-How-to-sniff-network-traffic> accessed 10 April 2017.

Cheung A.S.Y, 'Location privacy: The challenges of mobile service devices' (2014) Computer Law and Security Review 30 41.

Chirgwin R,'Telcos renew calls to limit metadata retention' *The Register* (London, 29 July 2014), <http://www.theregister.co.uk/2014/07/29/telcos_renew_calls_to_limit_metadata_retention/> accessed 17 April 2017.

Christl W, 'Corporate Surveillance in Everyday Life' (June 2017) <http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf> accessed 1 August 2018

-- 'How Companies Use Personal Data Against People' (October 2017) <http://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf> accessed 17 October 2017.

Christl W and Spiekermann S, *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy* (Facultas.Wuv Universitäts 2016), 25-118.

-- 'Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy'(2016) <http://www.privacylab.at/wp-content/uploads/2016/09/Christl-Networks__K_o.pdf> accessed 1 November 2016.

Citron D.K and Gray D.C, 'Addressing the Harm of Total Surveillance: a Reply to Professor Neil Richards' (2013) Harvard Law Review Forum 126 262.

Citron D.K and Pasquale F.A, 'The Scored Society: Due Process for Automated Predictions' (2014) Washington Law Review 89:1 1.

Claburn T, 'Rejecting Sonos' private data slurp basically bricks bloke's boombox' *The Register* (London, 11 October 2017) <https://www.theregister.co.uk/2017/10/11/sonos_privacy_speakers/> accessed 16 January 2018.

Clark B, 'Spotify is using billboards to call users out on their questionable listening habits' (30 November 2016) <http://thenextweb.com/music/2016/11/30/spotify-is-using-billboards-to-call-users-out-on-their-questionable-listening-habits/> accessed 4 December 2016.

Clarke C, 'Letter Jean Marie Cavada' (17 October 2005) <http://www.statewatch.org/news/2005/oct/data-ret-clarke-to-cavada-17-10-05.pdf> accessed 29 May 2017.

Clarke R, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms' (1997) <http://www.rogerclarke.com/DV/Intro.html> accessed 29 November 2016.

-- 'Data retention as mass surveillance: the need for an evaluative framework' (2015) International Data Privacy Law 5:2 121.

Clement A, Harkness J and Raine G, 'Metadata – both shallow and deep: the fraught key to big data mass state surveillance' (11 May 2016) <http://www.sscqueens.org/sites/default/files/8_clement_harkness_raine-metadata_-shallow_and_deep_-_bds_workshop_report_2016_may_11.pdf> accessed 13 October 2017.

Cobbe J, 'Casting the Dragnet: Communications Data Retention under the Investigatory Powers Act' (2017) <https://www.academia.edu/33709047/Casting_the_Dragnet_Communications_Data_Retention_under_the_Investigatory_Powers_Act> accessed 20 September 2017.

-- 'Casting the dragnet- communications data retention under the Investigatory Powers Act' (2018) Public Law 10.

Cole D, 'We Kill People Based on Metadata' *The New York Review of Books* (New York City, 10 May 2014) <http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/> accessed 9 April 2017.

Cole J and Stickings A, 'The Future of Crime Reporting' (2017) The RUSI Journal 162:1 68.

Comments on Research and Ad Targeting <https://newsroom.fb.com/news/h/comments-on-research-and-ad-targeting/> accessed 2 May 2017.

Commission, Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector' COM(2000) 385 final.

-- Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, COM (2005) 438 Final September 2005

-- 'Report from the Commission to the Council and the European Parliament Evaluation report on the Data Retention Directive (Directive 2006/24/EC)' (18 April 2011) COM(2011) 225 final.

-- 'Evidence for necessity of data retention in the EU' (March 2013) <http://www.statewatch.org/news/2013/aug/eu-com-mand-ret-briefing.pdf> accessed 6 June 2017.

-- 'Internet of Things – An action plan for Europe' (Communication) COM/2009/0278 final.

Committee on Civil Liberties, Justice and Home Affairs, 'Text of the compromise amendments' <https://drive.google.com/file/d/0Byeaj8v2GIOacnVwVlhqMWdUWFU/view> accessed 12 November 2017

Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes (4 June 2003) <http://www.statewatch.org/news/2003/jun/CommonIndustryPositionondataretention.pdf> accessed 25 May 2017.

Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of Regions: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM/2000/0890 final <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52000DC0890> accessed 25 May 2017.

Cooper D and Blaney R, 'E.U. Data Retention Proposals in the Headlines' (July 2005) <http://www.cov.com/files/Publication/47c9b539-a648-4028-8cea-bd226afe5f09/Presentation/PublicationAttachment/0ed397fe-42fe-4b03-be45-c03607e6f080/oid33931.pdf> accessed 25 May 2017.

Corfield G, 'TfL to track Tube users in stations by their MAC addresses' *The Register* (London, 17 November 2016) <http://www.theregister.co.uk/2016/11/17/tfl_to_track_tube_users_by_wifi_device_mac_address/> accessed 22 November 2016.

Council of Europe, 'Human Rights for Internet Users' <https://www.coe.int/en/web/internet-users-rights/guide> accessed 28 April 2017.

-- 'Guide on Article 6 of the European Convention on Human Rights - – Right to a fair trial (criminal limb)' (2014) <http://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf> accessed 15 May 2017.

Council of Europe's Commissioner for Human Rights, 'The rule of law on the Internet and in the wider digital world' (2014) <https://rm.coe.int/16806da51c> accessed 14 July 2017.

Council of Europe Committee of Experts, 'Study on the Human Rights Dimensions of Automated Data Processing Techniques (in particular algorithms) and possible Regulatory Implications' (6 October 2017) <https://rm.coe.int/study-hr-dimension-of-automated-data-processing-incl-algorithms/168075b94a> accessed 16 April 2018.

Council of Europe Research Division, 'Internet: case-law of the European Court of Human Rights' (June 2015) <http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf> accessed 8 May 2017.

Council of the European Union, Working Party on Telecommunications, Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, (16

November 2001) <http://www.statewatch.org/news/2001/nov/13883.pdf> accessed 23 May 2017.

-- Common Position adopted by the Council on 28 January 2002 with a view to the adoption of the Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, Statement of Reasons, (29 January 2002), <http://data.consilium.europa.eu/doc/document/ST-15396-2001-REV-2-ADD-1/en/pdf> accessed 23 May 2017.

-- 'EU Human Rights Guidelines on Freedom of Expression Online and Offline' (12 May 2014) <https://eeas.europa.eu/sites/eeas/files/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf> accessed 3 May 2017.

Council Resolution of 17th January 1995 on the lawful interception of telecommunications, OJ 1996 C 329/01 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:1996:329:FULL:EN:PDF> accessed 23 May 2017.

Cox J, 'Even the Food Standards Agency Could Access UK Surveillance Data Under New Bill' *Motherboard* (Montreal, 26 November 2015) <https://motherboard.vice.com/en_us/article/ezpddn/even-the-food-standards-agency-could-access-uk-surveillance-data-under-new-bill> accessed 27 November 2017.

Crassh, 'National Mass Communications Data Surveillance and the Law' (9 August 2016) <http://www.crassh.cam.ac.uk/blog/post/national-mass-communications-data-surveillance-and-the-law> accessed 27 November 2017.

Crawford K and Calo R, 'There is a Blind Spot in AI Research' (2016) Nature 538 311.

Crump C, 'Data Retention: Privacy, Anonymity, and Accountability Online' (2003) 56 Stan. L. Rev. 191.

Cryptmode, 'Best No Logs VPN' (25 March 2017) <https://cryptmode.com/best-no-logs-vpn/> accessed 25 April 2017.

Cuijpers C and Koops B-J, 'The 'smart meters' bill: a privacy test based on article 8 of the ECHR' (2008) <https://skyvisionsolutions.files.wordpress.com/2014/11/dutch-smart-meters-report-tilt-october-2008-english-version.pdf> accessed 9 December 2017.

-- 'Smart metering and privacy in Europe: lessons from the Dutch case' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds) *European Data Protection: Coming of Age* (Springer 2012).

-- 'Smart Metering and Privacy in Europe: Lessons from the Dutch Case' in Serge Gutwirth, Ronald Leenes, Paul de Hert, Yves Poulle (eds) *European Data Protection: Coming of Age* (Springer 2013)

Cunche M, 'I know your MAC address: targeted tracking of individual using Wi-Fi' (2014) Journal of Computer Virology and Hacking Techniques 10:4 <https://hal.inria.fr/hal-00858324/document> accessed 10 April 2017.

Custers B, Zarsky T and Schermer B, *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases (Studies in Applied Philosophy, Epistemology and Rational Ethics)* (Springer, Heidelberg 2013).

Dahan M, 'The Gaza Strip as Panopticon and Panspectron: The Disciplining and Punishing of a Society' (2013) IJEP 4:3 44.

Danezis G, 'UK Draft IP Bill: Who is a telecommunications operator?' (7 November 2015) <https://conspicuouschatter.wordpress.com/2015/11/07/uk-draft-ip-bill-who-is-a-telecommunications-operator/> accessed 5 December 2017.

-- 'What the CIA hack and leak teaches us about the bankruptcy of current "Cyber" doctrines' (8 March 2017) <https://www.benthamsgaze.org/2017/03/08/what-the-cia-hack-and-leak-teaches-us-about-the-bankruptcy-of-current-cyber-doctrines/> accessed 21 August 2017.

-- 'Traffic Data Retention Impact on civil society organizations' <https://pdfs.semanticscholar.org/8c8f/606fd68f661457011d611b6cf9ac8050f297.pdf> accessed 10 August 2017.

-- 'Covert Communications Despite Traffic Data Retention' <http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/cover.pdf> accessed 10 August 2017.

Davies S, 'Unlawful, unworkable, unnecessary' *The Guardian* (London, 13 July 2005) <https://www.theguardian.com/world/2005/jul/13/humanrights.july7> accessed 30 May 2017.

Davis J, '"Police Checkpoints on the Information Highway' (1994) Computer underground Digest 6:72.

Dearden L, 'Police accused of deploying facial recognition 'by stealth' in London' *The Independent* (London, 27 July 2018) <https://www.independent.co.uk/news/uk/crime/facial-recognition-uk-police-london-trial-data-human-rights-legal-action-met-a8466876.html> accessed 28 July 2018.

DeLanda M, *War in the Age of Intelligent Machines* (Swerwe Editions, New York, 1991).

Del Rey M, 'Internet Protocol, RFC 791' (1981) <http://www.rfc-editor.org/rfc/rfc791.txt> accessed 30 November 2017.

de Montjoye Y-A, Hidalgo C.A, Verleysen M and Blondel V.D, ' Unique in the Crowd: The privacy bounds of human mobility' (2013) Scientific Reports 3:1376 1.

Department for Digital, Culture, Media & Sport and Ed Vaizey, 'Manchester wins £10m prize to become world leader in 'smart city' technology' (3 December 2015)

<https://www.gov.uk/government/news/manchester-wins-10m-prize-to-become-world-leader-in-smart-city-technology> accessed 8 December 2017.

De Schutter O and Ringelheim J, 'Ethnic Profiling: A Rising Challenge for European Human Rights Law' (2008) Modern Law Review 71:3 358.

de Sola Pool I, *Technologies of Freedom* (Belknap Press; Reprint edition 1984).

Devlin H, 'AI programs exhibit racial and gender biases, research reveals' *The Guardian* (London, 13 April 2017) <https://www.theguardian.com/technology/2017/apr/13/ai-programs-exhibit-racist-and-sexist-biases-research-reveals> accessed 15 March 2018.

Dickman B.L, 'Untying Knotts: The Application of Mosaic Theory to GPS Surveillance in UNITED STATES V. MAYNARD' (2011) American University Law Review 60:3, 731.

Donaldson S, (10 April 2018) <https://twitter.com/sarah_donaldson/status/983651700270657536> accessed 16 April 2018.

Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offence including terrorism, Council doc. 8958/04, Brussels, 28 April 2004 <http://www.europarl.europa.eu/RegData/docs_autres_institutions/conseil/2004/08958/CONS_CONS(2004)08958_EN.doc> accessed 25 May 2017.

Dubber M.D and Valverde M, *The New Police Science: The Police Power in Domestic and International Governance* (Stanford University Press 2006).

Dutch Data Protection Authority, 'Microsoft Windows 10 Home and Pro investigation' (October 2017) https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/public_version_dutch_dpa_informal_translation_summary_of_investigation_report.pdf> accessed 13 October 2017.

Dwyer J, 'National Security Agency Said to Use Manhattan Tower as Listening Post' *The New York Times* (New York City, 17 November 2016) <http://www.nytimes.com/2016/11/18/nyregion/national-security-agency-said-to-use-manhattan-tower-as-listening-post.html?smid=tw-share&_r=0> accessed 20 November 2016.

Dzehtsiarou K, 'Comparative Law in the Reasoning of the European Court of Human Rights' (2010) University College Dublin Law Review 10 109.

EDPS, 'Press Statement: The CJEU rules that Data Retention Directive is invalid' (8 April 2014) <https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2014-08_press_statement_drd_en.pdf> accessed 12 June 2017.

-- 'Opinion 4/2015 Towards a New Digital Ethics Data, Dignity and Technology' <https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf> accessed 19 May 2017.

Edwards L, ‘Reconstructing Consumer Privacy Protection On-line: A Modest Proposal’ (2007) International Review of Law, Computers & Technology 18:3 313

-- Edwards, ‘Section 127 of the Communications Act 2003: Threat or Menace?’ (10 September 2012) <https://www.scl.org/articles/2579-section-127-of-the-communications-act-2003-threat-or-menace> accessed 1 December 2017.

-- ‘Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective’ (December 2015) <https://zenodo.org/record/34501/files/CREATe-Working-Paper-2015-11.pdf> accessed 1 August 2018.

Edwards L and Veale M, ‘Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For’ (2017) Duke Law & Technology Review 16:1 18

Encyclopaedia ‘Internet Applications’ <http://www.encyclopedia.com/computing/news-wires-white-papers-and-books/internet-applications> accessed 10 April 2017.

Englehardt S, Acar, G and Narayanan A, ‘No boundaries: Exfiltration of personal data by session-replay scripts’ (15 November 2017) <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/> accessed 15 November 2017.

Equipment Interference DRAFT Code of Practice, (2016).

Emmerson B and Mountfield H, ‘Opinion to the ICO’ (19 June 2002) <https://www.whatdotheyknow.com/request/127491/response/315758/attach/html/3/Counsels%20Opinion%20re%20The%20Telecommunications%20Regulations%201999%2019.6.02.pdf.html> accessed 22 August 2017

Ermert M, ‘EU Data retention might not be proportional to risks’ (9 July 2013) <https://policyreview.info/articles/news/eu-data-retention-might-not-be-proportional-risks/170> accessed 4 June 2017.

Escudero-Pascual A and Hosein G, ‘Questioning lawful access to traffic data’ (2004) Communications of the ACM 47:3 77.

Esman G, ‘Splunk and Tensorflow for Security: Catching the Fraudster with Behavior Biometrics’ (18 April 2017) <https://www.splunk.com/content/splunk-blogs/en/2017/04/18/deep-learning-with-splunk-and-tensorflow-for-security-catching-the-fraudster-in-neural-networks-with-behavioral-biometrics.html> accessed 24 April 2017.

European Commission, ‘Cookies’ <http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm> accessed 17 November 2016.

-- Legal analysis of a Single Market for the Information Society (SMART 2007/0037)’ (November 2009)

<http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7022&> accessed 6 December 2017.

-- 'Evaluation of Directive 2006/24/EC and of National Measures to Combat Criminal Misuse and Anonymous Use of Electronic Communications (DRAFT)', Room Document <http://www.vorratsdatenspeicherung.de/images/RoomDocumentEvaluationDirective200624EC.pdf> accessed 8 August 2017.

-- 'Evidence for necessity of data retention in the EU' (March 2013) <http://www.statewatch.org/news/2013/aug/eu-com-mand-ret-briefing.pdf> accessed 6 June 2017.

European Commission Legal Services Opinion, 'Committee on Civil Liberties, Justice and Home Affairs Legal Opinion - Question relating to the judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* - Directive 2006/24/EC on data retention - Consequences of the judgment' (2014) <http://www.statewatch.org/news/2015/apr/ep-ls-opinion-digital-rights-judgment.pdf> accessed 13 June 2017.

European Council (Art.50) (23 March 2018) - Draft guidelines.

European Court of Human Rights Factsheet – 'Protection of Reputation' (October 2017) http://www.echr.coe.int/Documents/FS_Reputation_ENG.pdf> accessed 8 November 2017.

European Digital Rights 'Shadow evaluation report on the Data Retention Directive (2006/24/EC)' (17 April 2011) <https://www.edri.org/files/shadow_drd_report_110417.pdf> accessed 12 August 2017.

European Parliament Committee on Civil Liberties, Justice and Home Affairs, 'Report on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism', A6-0174/2005 (31 May 2005) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A6-2005-0174+0+DOC+XML+V0//EN&language=bg> and <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0174+0+DOC+PDF+V0//EN> accessed 26 May 2017.

European Parliament, 'Surveillance and censorship: The impact of technologies on human rights' (2015) <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf> accessed 14 May 2017.

-- 'National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law' (2013) <http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf> accessed 14 November 2017.

-- Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, 21 February 2014 (2013/2188(INI)).

-- 'Regulating electronic communications A level playing field for telecoms and OTTs?' (September 2016) <http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/586641/EPRS_BRI%282016%29586641_EN.pdf> accessed 30 November 2017.

European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)) <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230> accessed 3 May 2017.

Eurostat, '1 in 10 EU businesses analyses big data' (16 May 2017) <http://ec.europa.eu/eurostat/web/products-eurostat-news/-/EDN-20170516-1?inheritRedirect=true&redirect=%2Feurostat%2F> accessed 27 October 2017.

Executive Summary of Privacy International and EDRi, 'Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention', (15 September 2004), <http://www.statewatch.org/news/2004/sep/data-retention.htm> accessed 29 May 2017.

Explanatory notes to the Communications Act 2003.

Explanatory notes to the Data Retention and Investigatory Powers Act 2014.

Explanatory notes to the Investigatory Powers Act 2016.

Explanatory notes to Regulation of Investigatory Powers Act 2000.

Evans R, 'BAE 'secretly sold mass surveillance technology to repressive regimes'' *The Guardian* (London, 15 June 2017) <https://www.theguardian.com/business/2017/jun/15/bae-mass-surveillance-technology-repressive-regimes> accessed 5 November 2017.

Eyal N, *Hooked: A Guide to Building Habit-Forming Products* (CreateSpace Independent Publishing Platform 2013).

Fabbrini F, 'Human Rights in the Digital Age The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.' (2015) Harvard Human Rights Journal 28 65.

Farahany N.A, 'Incriminating Thoughts' (2012) Stanford Law Review 64 351

Farand C, ''Worrying trend' of freedom of the press in the UK as country ranks 40 in latest Reporters Without Borders index' *The Independent* (London, 14 August 2017) <https://www.independent.co.uk/news/world/world-press-freedom-index-2017-reporters-without-borders-uk-freedom-information-a7893211.html> accessed 18 August 2017.

FDN, 'French Surveillance To Be Scrutinized By The European Court Of Justice' (July 2018) <https://www.fdn.fr/retention-des-donnees-conseil-etat-juillet2018/#magicdomid371> accessed 1 August 2018.

Feiler L, 'The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection' (2010) 1(3) EJLT <http://ejlt.org/article/view/29/75> accessed 25 October 2017.

Fenwick H, *Civil Liberties and Human Rights* (4th edn Routledge-Cavendish 2009).

Ferguson C, 'Do the police have the power to break up groups of innocent friends?' *The Guardian* (London, 19 March 2010) <https://www.theguardian.com/commentisfree/libertycentral/2010/mar/19/police-power-disperse-small-groups> accessed 11 November 2017.

Finch K and Tene O, 'Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town' (2015) Fordham Urban Law Journal 41:5 1581.

Fioretti J, 'EU court says mass data retention illegal' *Reuters* (London, 21 December 2016) <http://uk.reuters.com/article/uk-eu-court-privacy-idUKKBN14A0YD> accessed 21 June 2017.

Fioretti J and Volz D, 'Privacy group launches legal challenge against EU-U.S. data pact leftright 3/3leftright' *Reuters* (London, 27 October 2016) <http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN12Q2JK> accessed 2 November 2016.

Fischer C, 'Communications Network Traffic Data' (2010) <http://alexandria.tue.nl/extra2/689860.pdf> accessed 17 May 2017.

Fisher D, DeLine R, Czerwinski M and Drucker S, 'Interactions with Big Data Analytics' (2012) Interactions 19:3 50.

-- 'Communications Network Traffic Data: technical and legal aspects' (2010) Eindhoven: Technische Universiteit Eindhoven, 188.

Fisher J, 'The Draft Convention on Cybercrime: Potential Constitutional Conflicts' (2001) 32 U.West.L.A. L.Rev. 339.

Fiveash K, 'ISPs 'blindsided' by UK.gov's 'emergency' data retention and investigation powers law' *The Register* (London, 14 July 2014) <http://www.theregister.co.uk/2014/07/14/isps_blindsided_by_ukgovs_rushed_data_retention_and_investigation_powers_law/> accessed 3 December 2017.

Flexibility, 'Home is where the start-up is' <http://www.flexibility.co.uk/flexwork/location/home-enterprise.htm> accessed 30 November 2017.

Floridi L, 'A Look into the Future Impact of ICT on Our Lives' (2007) The Information Society 23:1 59.

-- *The Onlife Manifesto Being Human in a Hyperconnected Era* (Springer 2009).

-- 'On Human Dignity as a Foundation for the Right to Privacy' (2016) Philosophy & Technology 29:4.

Friedland G and Sommer R, 'Cybercasing the Joint: On the Privacy Implications of Geo-Tagging' (2010) <https://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf> accessed 14 April 2017.

Ford M, 'Article 8: Right to respect for private and family life (The implications on unfair dismissal)' (7 November 2014) <http://www.ier.org.uk/blog/article-8-right-respect-private-and-family-life-implications-unfair-dismissal> accessed 5 May 2017.

Ford R, 'Beware rise of Big Brother state, warns data watchdog' (16 August 2004) <https://www.thetimes.co.uk/article/beware-rise-of-big-brother-state-warns-data-watchdog-hhv3qtwgswk> accessed 3 January 2018.

Foster J.J, 'United States Mission to the European Union, Proposals For US-EU Counter-Terrorism Cooperation' (16 October 2001) <http://www.statewatch.org/news/2001/nov/06Ausalet.htm> accessed 23 May 2017.

Foucault M, *Discipline & Punish* (New York: Vintage 1977).

-- 'Sexuality and solitude' in Marshall Blonsky (ed) *On Signs: A Semiotics Reader* (Blackwell, Oxford).

Foundation for Information and Policy 'FIPR response to the retention of communications data consultation' <http://www.fipr.org/030530retention.html> accessed 12 August 2017.

Fuchs C, 'How can surveillance be defined?' (2011) Matrizes 5:1 109.

-- New Media, Web 2.0 and Surveillance' (2011) Sociology Compass 5:2 134.

-- 'Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society' (2012) <http://www.projectpact.eu/privacy-security-research-paper-series/%231_Privacy_and_Security_Research_Paper_Series.pdf> accessed 21 April 2017.

Fu K, Sit E, Smith K and Feamster N, 'Dos and Don'ts of Client Authentication on the Web' (2001) <http://static.usenix.org/publications/library/proceedings/sec01/full_papers/fu/fu_html/> accessed 10 April 2017.

Fura E and Klamberg M, 'The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA' in Josep Casadevall, Egbert Myjer, Michael O'Boyle (eds) *Freedom of Expression – Essays in honour of Nicolas Bratza – President of the European Court of Human Rights* (Wolf Legal Publishers, Oisterwijk 2012).

Fuster G.G, 'Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection' (2014) Birkbeck Law Review 2:2 263.

G8 Government Industry Workshop on Safety and Security in Cyberspace, (May 2001) <http://cryptome.org/g8-isp-e-spy.htm> accessed 23 May 2017.

Galetta A, 'The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?' (2013) European Journal of Law and Technology 4:2 <http://ejlt.org/article/view/221/377> accessed 16 May 2017.

Gallagher R and Moltke H, 'TITANPOINTE The NSA's Spy Hub in New York, Hidden in Plain Sight' *The Intercept* (16 November 2016) <https://theintercept.com/2016/11/16/the-nsas-spy-hub-in-new-york-hidden-in-plain-sight/> accessed 17 November 2016.

García S and Luengo J, 'Tutorial on practical tips of the most influential data preprocessing algorithms in data mining' (2016) Knowledge-Based-Systems 98 1.

Garrie D.B and Wong R, 'Privacy in electronic communications: the regulation of VoIP in the EU and the United States' (2009) C.T.L.R. 15:6 139

Gasper R, NCIS submission on data retention law: Looking to the future – clarity on communications data retention law' (21 Aug 2000) <https://cryptome.org/ncis-carnivore.htm> accessed 26 May 2017.

Gasson M.N, Kosta E, Royer D, Meints M, and Warwick K, 'Normality Mining: Privacy Implications of Behavioral Profiles Drawn from GPS Enabled Mobile Phones' (2011) IEEE Transactions on Systems, Man and Cybernetics 41:2 251.

Gayle D, ''Downward spiral': UK slips to 40th place in press freedom rankings' *The Guardian* (London, 26 April 2017) <https://www.theguardian.com/media/2017/apr/26/uk-world-press-freedom-index-reporters-without-borders> accessed 13 November 2017.

Geert K, 'On presuming innocence' (2013) Neth J Leg Philos 42:3 225.

Gerards J, 'The Discrimination Grounds of Article14 of the European Convention on Human Rights' (2013) Human Rights Law Review 13:1 99.

German Forsa Institute, 'Meinungen der Bunderburger zur Vorratsdatanspeicherung' (28 May 2008) <http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf> accessed 26 April 2017.

Gershgorn D, 'Google explains how artificial intelligence becomes biased against women and minorities' (28 August 2017) <https://qz.com/1064035/google-goog-explains-how-artificial-intelligence-becomes-biased-against-women-and-minorities/> accessed 15 March 2018.

Ghosh D and Scott B, 'Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You' *Time* (New York City, 19 March 2018)

<http://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/> accessed 16 April 2018.

Giddens A, *The Nation State and Violence: Volume Two of a Contemporary Critique of Historical Materialism* (Cambridge: Polity Press),

Golubovic D, 'Freedom of association in the case law of the European Court of Human Rights' (2013) The International Journal of Human Rights, 17:7-8 758.

González Casanova P, *Latin America Today* (United Nations University Press 1993).

Gonza´lez M.C, Hidalgo C.A and Baraba´si A-L, 'Understanding individual human mobility patterns' (2008) Nature 453 779.

Goold B.J, 'Surveillance and the Political Value of Privacy' (2009) Amsterdam Law Forum 3 1:4.

Gordon D.R, 'The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System' (1987) Politics & Society December 15:4 483.

Gorman C, 'The Mind-Reading Machine' (9 July 2012) <https://spectrum.ieee.org/biomedical/diagnostics/the-mindreading-machine> accessed 9 November 2017.

Grace J, 'Clare's Law, or the national Domestic Violence Disclosure Scheme: the contested legalities of criminality information sharing' (2015) The Journal of Criminal Law, 79:1.

Graham S, 'Bridging Urban Digital Divides? Urban Polarisation and Information and Communications Technologies (ICTs)' (2002) Urban Studies 39:1 33.

Grandy O, *The panoptic sort. A political economy of personal information* (Boulder: Westview Press 1993).

Granger M-P 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) European Law Review 39:6 835.

Greer S, 'The Margin of Appreciation: Interpretation and Discretion under the European Convention on Human Rights' (2000) <https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17(2000).pdf> accessed 2 March 2018.

Griffin A, 'How Facebook Is Manipulating You to Vote' *The Independent* (London, 5 May 2016) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/uk-elections-2016-how-facebook-is-manipulating-you-to-vote-a7015196.html> accessed 16 April 2018.

Gullo K, 'Surveillance Chills Speech—As New Studies Show—And Free Association Suffers' (19 May 2016) <https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-free-association> accessed 12 May 2017.

Gunelius S, 'The Data Explosion in 2014 Minute by Minute – Infographic' (12 July 2014) <https://aci.info/2014/07/12/the-data-explosion-in-2014-minute-by-minute-infographic/> accessed 27 October 2017.

Hadjimatheou K, 'Surveillance, the moral presumption of innocence, the right to be free from criminal stigmatisation and trust' (2013) <https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D4.5-Surveillance-the-moral-presumption-of-innocence.pdf> accessed 16 May 2017.

-- 'The Relative Moral Risks of Untargeted and Targeted Surveillance' (2014) Ethic Theory Moral Prac 17 187.

-- 'Surveillance Technologies, Wrongful Criminalisation, and the Presumption of Innocence' (2016) Philosophy & Technology <http://wrap.warwick.ac.uk/79568/1/WRAP_art%253A10.1007%252Fs13347-016-0218-2_.pdf> accessed 16 May 2017.

Haggerty K.D and Gazso A, 'Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats' (2005) The Canadian Journal of Sociology 30:2 169.

Haggerty K.D and Samatas M, 'Surveillance and democracy: an unsettled relationship' in Kevin D. Haggerty and Mina Samatas (eds), *Surveillance and Democracy* (Routledge-Cavendish (2010),

Hansen, 'Data Preservation: An Effective Approach to Combating Internet Crime in the UK' (2003) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=947371> accessed 12 August 2017.

Harcourt B.E, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* (Chicago: University of Chicago Press 2007).

Harlow C, 'Surveillance and the Superstate' (2 May 2012) <http://ukconstitutionallaw.org/2012/05/02/carol-harlow-surveillance-and-the-superstate/> accessed 3 December 2017.

Harris R, 'More data will be created in 2017 than the previous 5,000 years of humanity' (23 December 2016) <https://appdevelopermagazine.com/4773/2016/12/23/more-data-will-be-created-in-2017-than-the-previous-5,000-years-of-humanity-/> accessed 27 October 2017.

Hart D, 'A1P1 claims by photovoltaics get to the Court of Appeal' (4 May 2015) <https://ukhumanrightsblog.com/2015/05/04/a1p1-claims-by-photovoltaics-gets-to-the-court-of-appeal/> accessed 16 April 2018.

Hayward, 'How to use OneDrive: A guide to Microsoft's cloud storage solution' (14 February 2016) <http://www.trustedreviews.com/how-to/how-to-use-onedrive-2945212> accessed 3 December 2017.

HC Deb 14 July, vol 584.

HC Deb 4 November 2015, vol 601.

Hern A, 'State hackers 'probably compromised' energy sector, says leaked GCHQ memo' *The Guardian* (London, 18 July 2017) <https://www.theguardian.com/technology/2017/jul/18/energy-sector-compromised-state-hackers-leaked-gchq-memo-uk-national-cybersecurity-centre> accessed 21 August 2017.

-- 'UK homes vulnerable to 'staggering' level of corporate surveillance' *The Guardian* (London, 1 June 2018) <https://www.theguardian.com/technology/2018/jun/01/uk-homes-vulnerable-to-staggering-level-of-corporate-surveillance> accessed 17 June 2018.

Hewitt P, and Clarke C, Joint letter to Independent on Sunday, 28 Jan 2000.

Hickman T, 'Proportionality: Comparative Law Lessons' (2007) 12 Jud. Rev. 31.

Higgs E, 'The Rise of the Information State: the Development of Central State Surveillance of the Citizen in England, 1500–2000' (2001) Journal of Historical Sociology 14 :2 175.

Hintz A and Dencik L, 'The politics of surveillance policy: UK regulatory dynamics after Snowden' (2016) Internet Policy Review 5:3 1.

HL Deb 27 November 2001 vol 629.

-- 4 Dec vol 629.

-- 12 September 2016, vol 774.

HM Government, 'The exchange and protection of personal data: A FUTURE PARTNERSHIP PAPER' (27 August 2017) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf> accessed 9 April 2018.

Hoffman C, 'How (and Why) to Change Your MAC Address on Windows, Linux, and Mac' (30 June 2014) <https://www.howtogeek.com/192173/how-and-why-to-change-your-mac-address-on-windows-linux-and-mac/> accessed 11 April 2017.

Holmes Jr O.W, 'The Path of the Law' (1897) Harv L Rev 10:8 457.

Home Affairs Committee, *UK-EU security cooperation after Brexit (fourth report)* (2017-19 HC 635).

Home Office, 'Retention of Communications Data Under Part 11: Anti-terrorism, Crime and Security Act 2001, Voluntary Code of Practice' <http://www.opsi.gov.uk/si/si2003/draft/5b.pdf> accessed 30 November 2017.

-- 'Protecting the Public in a Changing Communications Environment' (2009) <http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/27_04_09communicationsconsultation.pdf> accessed 29 July 2017.

-- 'Protecting the Public in a Changing Communications Environment, Summary of Responses to the 2009 Consultation

Paper'<http://webarchive.nationalarchives.gov.uk/+/http:/www.homeoffice.gov.uk/documents/cons-2009-communication-data/cons-2009-comms-data-responses2835.pdf?view=Binary> accessed 12 October 2017.

-- *Draft Communications Data Bill* (Cm 8359, 2012).

-- *Draft Investigatory Powers Bill* (Cm 9152 2015).

-- 'Acquisition and Disclosure of Communications Data Code of Practice' (March 2015) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf> accessed 30 November 2017.

-- 'Communications data' (17 March 2015) < https://www.gov.uk/government/collections/communications-data> accessed 3 April 2017.

'Operational Case for the Retention of Internet Connection Records' (1 March 2016) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504192/Operational_Case_for_the_Retention_of_Internet_Connection_Records_-_IP_Bill_introduction.pdf> accessed 29 July 2017.

-- 'Investigatory Powers Act 2016 Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data' (November 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663668/November_2017_IPA_Consultation_-_consultation_document.pdf> accessed 5 January 2018.

-- 'Open consultation Investigatory Powers Act 2016' (30 November 2017) <https://www.gov.uk/government/consultations/investigatory-powers-act-2016> accessed 15 January 2018.

-- 'Investigatory Powers Act 2016' (30 November 2017) <https://www.gov.uk/government/consultations/investigatory-powers-act-2016> accessed 11 December 2017.

-- 'Communications Data DRAFT Code of Practice' (November 2017) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/663675/November_2017_IPA_Consultation_-_Draft_Communications_Data_Code_of_Pract....pdf> accessed 16 January 2018.

-- 'Investigatory Powers Act 2016: Response to Home Office Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data' (June 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/724142/June_2018_IPA_regulations_-_Government_Response_to_consultation_on_response_to_ECJ_judgment.pdf> accessed 1 August 2018.

Hookway B, *Pandemonium: The rise of predatory locales in the postwar world* (Princeton, N.J.: Princeton Architectural Press 2000).

Horowitz M, 'Defending your router, and your identity, with a password change' (19 March 2008) <https://www.cnet.com/uk/news/defending-your-router-and-your-identity-with-a-password-change/> accessed 10 April 2017.

Hotz R.L, 'The Really Smart Phone' *Wall Street Journal* (New York City, 23 April 2011) <https://www.wsj.com/articles/SB10001424052748704547604576263261679848814> accessed 14 April 2017.

Houpert J.F, 'What You Need To Know About 1st, 2nd and 3rd Party Data' (20 June 2017) <https://www.datacratic.com/blog/first-second-third-party-data> accessed 10 October 2017.

House of Commons Library, 'Brexit: what happens next?' (30 June 2016) <http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7632> accessed 25 July 2016.

House of Lords European Union Committee, *Brexit: the EU data protection package (third report)* (2017-19 HL 7).

-- *The UK, the EU and a British Bill of Rights; (12th Report)* (2015-16 HL 139).

House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State. Volume I: Report* (second report) (2008–09, HL 18–I).

Hoyano L, 'What is balanced on the scales of justice? In search of the essence of the right to a fair trial' (2014) Crim. L.R. 1 4.

Hu W-C, *Multidisciplinary Perspectives on Telecommunications, Wireless Systems, and Mobile Computing* (IGI Global 2013).

Hughes K, 'The social value of privacy, the value of privacy to society and human rights discourse' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy Interdisciplinary Perspectives* (Cambridge University Press 2015).

Humphries M, 'Facebook stores up to 800 pages of personal data per user account' (28 September 2011) <https://www.geek.com/geek-pick/facebook-stores-up-to-800-pages-of-personal-data-per-user-account-1424807/> accessed 30 October 2017.

Humphreys S and de Zwart M, 'Data retention, journalist freedoms and whistleblowers' (2017) Media International Australia 165:1 103.

Husovec M, 'First European Constitutional Court Suspends Data Retention after the Decision of the Court of Justice of EU' (29 April 2014) <https://cyberlaw.stanford.edu/blog/2014/04/first-european-constitutional-court-suspends-data-retention-after-decision-court> accessed 14 June 2017.

Hustinx P, 'The "moment of truth" for the Data Retention Directive: EDPS demands clear evidence of necessity' (3 December 2010) <http://europa.eu/rapid/press-release_EDPS-10-17_en.htm?locale=en> accessed 25 May 2017.

Hyde R and Savage A, 'Cross-border Concerns: Perils and Possibilities' (2013) E-Journal of International and Comparative LABOUR STUDIES 2:3 <http://ejcls.adapt.it/index.php/ejcls_adapt/article/viewFile/132/195> accessed 5 May 2017.

ICO Enforcement Notice (23 July 2012) <http://breachwatch.com/wp-content/uploads/2012/08/Southampton-County-Council-Enforcement-Notice.pdf> accessed 22 August 2017.

-- (15 July 2013) <http://breachwatch.com/wp-content/uploads/2013/07/hertfordshire-constabulary-enforcement-notice.pdf> accessed 22 August 2017.

ICO News, 'Privacy regulators study finds Internet of Things shortfalls' (22 September 2016) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/09/privacy-regulators-study-finds-internet-of-things-shortfalls/> accessed 22 September 2016.

Ienca M, 'Do We Have a Right to Mental Privacy and Cognitive Liberty?' (3 May 2017) <https://blogs.scientificamerican.com/observations/do-we-have-a-right-to-mental-privacy-and-cognitive-liberty/> accessed 11 October 2017.

Ienca M and Andorno R, 'Towards new human rights in the age of neuroscience and neurotechnology' (2017) Life Sciences, Society and Policy 13:5 1.

IJClark, 'Digital privacy and digital citizens' (16 September 2016) <http://infoism.co.uk/2016/09/digital-citizens/> accessed 1 November 2016.

iiNet, 'Limited Submission to the Committee' <http://www.aph.gov.au/DocumentStore.ashx?id=cd64d063-5791-4336-8606-0ee36926b8f9&subId=206461> accessed 17 April 2017.

-- Protecting your privacy: Our stand against 'mandatory data retention'' (21 July 2014) <http://blog.iinet.net.au/protecting-your-privacy/> accessed 30 December 2016.

ILETS Report (1999) <http://www.statewatch.org/news/2001/may/ILETS99-report.doc> accessed 23 May 2017.

Information Commissioner's Office, 'Key concepts and definitions' <https://ico.org.uk/for-organisations/guide-to-pecr/key-concepts-and-definitions/> accessed 1 December 2017.

-- 'Big data, artificial intelligence, machine learning and data protection' (2017) <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed 15 March 2018.

Informm, 'Case Law: Chambers v DPP, "Twitter joke" case, appeal successful' (29 July 2012) <https://inforrm.wordpress.com/2012/07/29/case-law-chambers-v-dpp-twitter-joke-case-appeal-successful/> accessed 1 December 2017.

Institute For Prospective Technological Studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*: Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs, European Communities (2003) <http://ftp.jrc.es/EURdoc/eur20823en.pdf> accessed 12 August 2017.

Intelligence and Security Committee, 'About the Committee' <http://isc.independent.gov.uk/> accessed 31 May 2018.

-- *Privacy and Security: A modern and transparent legal framework* (2014, HC 1075).

-- *Report on the draft Investigatory Powers Bill*, (2016, HC 795).

Interception of Communications Commissioner 'IOCCO inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources' (4 February 2015) <http://www.iocco-uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf> accessed 6 April 2017.

Investigatory Powers Bill European Convention on Human Rights Memorandum <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473763/European_Convention_on_Human_Rights_Memorandum.pdf> accessed 6 March 2018.

Investigatory Powers Bill, Internet Connection Records, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473745/Factsheet-Internet_Connection_Records.pdf> accessed 17 April 2017.

Investigatory Powers Bill HL Bill (2016-17) 40—VI 56/2.

Investigatory Powers Bill Written evidence submitted by Adrian Kennard (IPB 13) (March 2016) <http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB13.htm> accessed 11 December 2017.

Investigatory Powers Commissioner Office, 'Approval of Warrants, Authorisations and Notices by Judicial Commissioners' (March 2018) <http://www.ipco.org.uk/docs/20180308_IPCO%20Advisory%20Notice%2012018.pdf> accessed 13 March 2018.

Irion K, 'Accountability unchained: Bulk Data Retention, Preemptive Surveillance, and Transatlantic Data Protection' in Marc Rotenberg, Julia Horwitz and Jeramie Scott (eds), *Privacy in the Modern Age The Search for Solutions* (New Press 2015).

IT-Pol, 'Denmark allows massive retention of location data for mobile internet' (28 June 2017) <https://edri.org/denmark-allows-massive-retention-of-location-data-for-mobile-internet/> accessed 11 August 2017.

-- 'EU Member States plan to ignore EU Court data retention rulings' (29 November 2017) <https://edri.org/eu-member-states-plan-to-ignore-eu-court-data-retention-rulings/> accessed 15 January 2018.

Jackson M, 'UK ISP BT Tops 9 Million Broadband Users, 4.1M on Superfast Fibre FTTC' (5 May 2016) <http://www.ispreview.co.uk/index.php/2016/05/uk-isp-bt-top-9-million-broadband-users-4-1m-fibre-broadband.html> accessed 15 August 2017.

Jacobs B, 'Keeping our Surveillance Society Nontotalitarian' (2009) 1(4) Amsterdam Law Forum <http://amsterdamlawforum.org/article/view/91/165> accessed 3 January 2018.

Jacobs I and Walsh N, 'Architecture of the World Wide Web, Volume One' (15 December 2004) <http://www.w3.org/TR/webarch/> accessed 5 December 2017.

Jay R, 'The Data Retention and Investigatory Powers Act 2014 – Recent Developments' (15 January 2015) <https://www.scl.org/articles/3279-the-data-retention-and-investigatory-powers-act-2014-recent-developments> accessed 3 December 2017.

Jeong S, 'Terror Scanning Database For Social Media Raises More Questions than Answers' *Motherboard* (Montreal, 9 December 2016) <https://motherboard.vice.com/read/social-media-terror-scanning-database> accessed 21 December 2016.

Johnson A.N, 'Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity' (2001) European Journal of Social Psychology 31 177.

Johnson P, 'Sociology and the European Court of Human Rights' (2014) Sociological Review 62:3 547.

Joint Committee on Human Rights, *First Report* (2000-01), HL 42/HC 296).

-- *Legislative Scrutiny: Draft Voluntary Code of Practice on Retention of Communications Data under Part 11 of the Anti-terrorism, Crime and Security Act 2001* (*sixteenth report*) (2002-03, HL 181, HC 1272) 19.

Joint Committee on the Draft Communications Data Bill, *Draft Communications Data Bill*, (2012-2013 HL 79 HC 479).

Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill* (2015-16, HL 93, HC 651) 123.

-- *written evidence*, (February 2016), <http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf> accessed 5 April 2017.

-- *oral evidence*, <https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf> accessed 29 April 2017.

Jones C and Hayes B, 'The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy' (2013), <http://www.statewatch.org/news/2013/dec/secile-data-retention-directive-in-europe-a-case-study.pdf> accessed 23 May 2017

JUSTICE, 'Freedom from Suspicion Surveillance Reform for a Digital Age' (October 2011) <http://www.statewatch.org/news/2011/nov/uk-ripa-justice-freedom-from-suspicion.pdf> accessed 04 October 2016.

Kaflan C.S, 'Kafkaesque? Big Brother? Finding the Right Literary Metaphor for Net Privacy' *The New York Times* (New York City, 2 February 2001) <http://www.nytimes.com/2001/02/02/technology/kafkaesque-big-brother-finding-the-right-literary-metaphor-for.html> accessed 17 January 2018.

Kalmanek, Sudip Misra, Yang Richard Yang, *Guide to Reliable Internet Services and Applications* (Springer Science & Business Media 2010).

Karemba B, 'The Investigatory Powers Bill: Putting the Investigatory Powers Commissioner in Focus (Part II)' (15 April 2016) <https://ukconstitutionallaw.org/2016/04/15/byron-karemba-the-investigatory-powers-bill-putting-the- investigatory-powers-commissioner-in-focus-part-ii/> accessed 13 July 2017.

Kaye D, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (22 May 2015) Human Rights Council, U.N. Doc.A/HRC/29/32 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement> accessed 28 April 2017.

-- 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (11 May 2016) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/12/PDF/G1609512.pdf?OpenElement> accessed 4 May 2017.

Kelion L, 'Tech firms seek to frustrate internet history log law' *BBC News* (London, 23 November 2016) <http://www.bbc.co.uk/news/technology-38068078> accessed 30 July 2017.

-- Kelion, 'TalkTalk's wi-fi hack advice is 'astonishing'' *BBC News* (London, 7 December 2016) <http://www.bbc.co.uk/news/technology-38223805> accessed 21 August 2017.

Kentish B, 'Brexit: MPs vote against including European fundamental rights charter in UK law' *The Independent* (London, 16 January 2018) <https://www.independent.co.uk/news/uk/politics/brexit-mps-vote-against-including-european-fundamental-rights-charter-in-uk-law-a8162981.html> accessed 16 January 2018

-- 'House of Lords defeats government plans to scrap EU rights charter after Brexit' *The Independent* (London, 23 April 2018) <https://www.independent.co.uk/news/uk/politics/brexit-latest-eu-rights-charter-uk-government-house-of-lords-withdrawal-bill-a8318731.html> accessed 31 May 2018.

OthmanThani S.K.S, Mohd N.H. Hashim and Ismail W.H.W, 'Surveillance by Design: Assessment using principles of Crime Prevention through Environmental Design (CPTED) in urban parks' (2016) Elsevier Procedia - Social and Behavioral Sciences 234 506.

Kift P and Nissenbaum H, 'Metadata in Context - An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program' (2017) ISJLP 13 333.

Kilkelly U, 'A guide to the implementation of Article 8 of the European Convention on Human Rights' (August 2003) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168007ff47> accessed 26 April 2017.

Killock J, 'ISPs will break the law if they continue to retain our data' (9 April 2014) <https://www.openrightsgroup.org/blog/2014/are-the-government-and-isps-breaking-the-law-by-continuing-to-retain-our-data> accessed 23 May 2017.

Kim S, 'ECHR Jurisdiction and Mass Surveillance: Scrutinising the UK Investigatory Power Tribunal's Recent Ruling' (9 June 2016) <https://www.ejiltalk.org/echr-jurisdiction-and-mass-surveillance-scrutinising-the-uk-investigatory-power-tribunals-recent-ruling/> accessed 6 May 2017.

Kirby M, 'Australia's Growing Debt to the European Court of Human Rights' (2008) Monash University Law Review 34:2 239.

Kirkpatrick M, 'Google CEO Schmidt: "People Aren't Ready for the Technology Revolution"' (4 August 2010) <http://readwrite.com/2010/08/04/google_ceo_schmidt_people_arent_ready_for_the_tech/> accessed 4 December 2016.

Kitchin R, 'Getting smarter about smart cities: Improving data privacy and data security' (2016) <http://www.taoiseach.gov.ie/eng/Publications/Publications_2016/Smart_Cities_Report_January_2016.pdf> accessed 2 September 2017.

-- 'Continuous Geosurveillance in the "Smart City"' <http://dismagazine.com/dystopia/73066/rob-kitchin-spatial-big-data-and-geosurveillance/> accessed 4 September 2017.

Kobe N, 'Blow for Snoopers Charter as EU court bans mass data collection' *ITPro* (21 December 2016) <http://www.itpro.co.uk/public-sector/snoopers-charter/27819/blow-for-snoopers-charter-as-eu-court-bans-mass-data-collection> accessed 21 June 2017.

Koerner R, 'Privacy vs. Security: A False Dichotomy' *HuffPost* (5 April 2014), <http://www.huffingtonpost.com/robin-koerner/privacy-vs-security-a-fal_b_4698157.html> accessed 7 March 2017.

Kokott J and Sobotta C, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) International Data Privacy Law 3:4 222.

Konstadinides T, 'Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem' (2011) E.L. Rev. 36:5 722.

-- 'Mass Surveillance and Data Protection in EU Law: The Data Retention Directive Saga' in Maria Bergström and Anna Jonsson Cornell (ed) *European Police and Criminal Law Co-Operation* (Swedish Studies in European Law (5), Hart Publishing, Oxford, 2014).

Korff D, 'The Standard Approach Under Articles 8-11 ECHR and Article 2 ECHR' (2009) <http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf> accessed 5 November 2017.

-- 'Passenger Name Records, data mining & data protection: the need for strong safeguards' (15 June 2015) <https://rm.coe.int/16806a601b> accessed 6 November 2017.

-- 'We can use European law to challenge this spying' (23 June 2013) <https://www.theguardian.com/commentisfree/2013/jun/23/european-law-challenge-surveillance-human-rights> accessed 9 November 2017.

Koskela H, 'Cam Era' – the contemporary urban Panopticon' (2003) Surveillance & Society 1:3 292.

Kosta E, 'The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection' (2013) SCRIPTed 10:3 339.

Kotschy W, 'The proposal for a new General Data Protection Regulation—problems solved?' (2014) International Data Privacy Law 4:2 274.

Koopman C, 'The Power Thinker' (15 March 2017) <https://aeon.co/essays/why-foucaults-work-on-power-is-more-important-than-ever?utm_content=buffer25bb6&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer> accessed 8 January 2018.

Knyrim R and Trieb G, 'Smart metering under EU data protection law' (2011) International Data Privacy Law 1:2.

Kramera A.D.I, Guillory J.E, and Hancockb J.T, 'Experimental evidence of massive-scale emotional contagion through social networks' (2014) 111:24 8788.

Kravets D, 'Maker of Internet of Things-connected vibrator will settle privacy suit' *Ars Technica* (8 December 2016) <http://arstechnica.com/tech-policy/2016/12/maker-of-internet-of-things-connected-vibrator-will-settle-privacy-suit/> accessed 18 December 2016.

Kühlewind M, Kutscher D and Trammell B, 'Enabling Traffic Management without DPI' (2015) <https://www.iab.org/wp-content/IAB-uploads/2015/08/MaRNEW_1_paper_18.pdf> accessed 17 April 2017.

Lace S, 'The new personal information agenda' in Susanne Lace (ed) *The Glass Consumer* (Birstol: Policy Press 2005).

Lanier J, 'Should Facebook Manipulate Users?' *The New York Times* (New York City, 30 June 2014) <https://www.nytimes.com/2014/07/01/opinion/jaron-lanier-on-lack-of-transparency-in-facebook-study.html> accessed 25 November 2017.

Lapidos J, 'The Undemocratic People's Republic of Korea' *Slate* (New York City, 1 April 2009) <http://www.slate.com/articles/news_and_politics/explainer/2009/04/the_undemocratic_peoples_republic_of_korea.html> accessed 4 January 2018.

La Rue R, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (17 April 2013) <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf> accessed 3 May 2017.

Law Society and Bar Council, 'Investigatory Powers and Legal Professional Privilege' (2015) <https://www.lawsociety.org.uk/news/documents/position-paper-investigatory-powers-legal-professional-privilege-october-2015/> accessed 17 May 2017.

Ledvina A, '10 ways Facebook is actually the devil' (4 July 2014) <http://andrewledvina.com/code/2014/07/04/10-ways-facebook-is-the-devil.html> accessed 25 November 2017

Lee A, 'Beyond metadata: the brave new world of big data retention' *The Conversation* (Melbourne, 31 March 2015) <https://theconversation.com/beyond-metadata-the-brave-new-world-of-big-data-retention-38720> accessed 13 October 2017

Lee A and Cook P, 'Seeing through the PRISM: the history of everyday surveillance' *The Conversation* (Melbourne, June 2013) <http://theconversation.com/seeing-through-the-prism-the-history-of-everyday-surveillance-15139> accessed 1 November 2016.

Lee T, 'Singapore an advanced surveillance state, but citizens don't mind' *TechCrunch* (Bay Area, 26 November 2013) <https://www.techinasia.com/singapore-advanced-surveillance-state-citizens-mind> accessed 2 November 2016.

Legal Services letter to Permanent Representatives Committee, Brussels, 1 February 2017 (OR. en) 5884/17.

Le Nouaille D, 'Instagram is listening to you' *The Medium* (25 August 2017) <https://medium.com/@damln/instagram-is-listening-to-you-97e8f2c53023> accessed 1 November 2017.

Lesta G, *A Theory of Interpretation of the European Convention on Human Rights* (Oxford University Press, 2007).

Levi M and Wall D.S, 'Technologies, Security, and Privacy in the Post-9/11 European Information Society' (2004) Journal of Law and Society 31:2 194.

Liao L, Patterson D.J, Fox D and Kautz H, 'Building Personal Maps from GPS Data' (2006) Ann. New York Acad. Sci 1093:1 249.

Liberty, 'State Surveillance' <https://www.liberty-human-rights.org.uk/human-rights/privacy/state-surveillance> accessed 3 January 2018.

-- 'Liberty's Submission to the Joint Committee on the Draft Communications Data Bill' (August 2012) <http://www.liberty-human-rights.org.uk/pdfs/policy12/liberty-submission-to-the-draft-communications-data-bill-committee-aug-2012-.pdf> accessed 24 August 2017.

-- 'Liberty's briefing on 'A Question of Trust: The Report of the Investigatory Powers Review'' (June 2015) <https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%27s%20response%20to%20A%20Question%20of%20Trust%20-%20the%20report%20of%20the%20investigatory%20powers%20review_1.pdf> accessed 1 August 2017.

-- 'Liberty's briefing on 'Internet Connection Records' in the Investigatory Powers Bill for Report Stage in the House of Lords' (October 2016) <https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%20briefing%20on%20ICRs%20for%20Report%20Stage%20in%20the%20House%20of%20Lords.pdf> accessed 10 October 2017.

-- 'Government IS breaking the law by collecting everyone's internet and call data and accessing it with no independent sign-off and no suspicion of serious crime' (21 December 2016) <https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/government-breaking-law-collecting-everyones-internet-and-call> accessed 21 June 2017.

Lightfoot G and Wisniewski T.P, 'Information asymmetry and power in a surveillance society' (2014) Information and Organization 24 214.

Lin Y-D, Tseng K-K, Lee T-H, Lin Y-N, Hung C-C and Lai Y-C, 'A platform-based SoC design and implementation of scalable automaton matching for deep packet inspection' (2007) Journal of Systems Architecture 53 937.

Lipof, R. 'Boardwatch' (1999) 13:12 94.

Littler A, *Member States versus the European Union: The Regulation of Gambling* (Martinus Nijhoff Publishers 2011).

Locke C, 'A Rare Look at the Archives of the German Secret Police' *Wired* (San Francisco, California, 11 June 2017) <https://www.wired.com/2017/05/adrian-fish-the-stasi-archives/> accessed 4 January 2018.

Logan J, 'The Electronic Police State: 2008 National Rankings' (2008) <https://secure.cryptohippie.com/pubs/EPS-2008.pdf> accessed 4 January 2018.

-- 'The Electronic Police State: 2010 National Rankings' (2010) <https://secure.cryptohippie.com/pubs/EPS-2008.pdf> accessed 4 January 2018.

Loideain N, 'EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era' (2015) Media and Communication 3:2 53.

-- , 'The UK Investigatory Powers Bill – one step forward, two steps back' *openDemocracy* (17 November 2015) <https://www.opendemocracy.net/digitaliberties/nora-ni-loideain/uk-investigatory-powers-bill-one-step-forward-two-steps-back> accessed 7 August 2017.

-- 'Written evidence' (2016) <https://publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB64.pdf> accessed 1 August 2017.

Lomas N, 'UK surveillance bill includes powers to limit end-to-end encryption' *TechCrunch* (Bay Area, June 2016) <https://techcrunch.com/2016/07/15/uk-surveillance-bill-includes-powers-to-limit-end-to-end-encryption/> accessed 26 November 2016.

-- 'Windows 10 privacy settings still worrying European watchdogs' *TechCrunch* (Bay Area, 21 February 2017) <https://techcrunch.com/2017/02/21/windows-10-privacy-settings-still-worrying-european-watchdogs/> accessed 24 April 2017.

Lumb T, 'New Microsoft research: technology and the home' (28 October 2013) <https://www.marketingsociety.com/the-library/new-microsoft-research-technology-and-home> accessed 8 November 2017.

Lundin L, 'PINs and Passwords, Part 2' (11 August 2013) <http://www.sleuthsayers.org/2013/08/pins-and-passwords-part-2.html> accessed 10 April 2017.

Lynskey O, 'Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order' (2014) ICLQ 63:3 569.

-- 'Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Other*: The Good, the Bad and Ugly' (8 April 2014) <http://europeanlawblog.eu/2014/04/08/joined-cases-c-29312-and-59412-digital-rights-ireland-and-seitlinger-and-others-the-good-the-bad-and-the-ugly/> accessed 13 June 2017.

-- 'The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: *Digital Rights Ireland*' (2014) Common Market Law Review 51: 1789.

Lyon D, 'From Big Brother to Electronic Panopticon' in David Lyon (ed) *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis: University of Minnesota Press, 1994)

-- *Surveillance society: monitoring everyday life* (Buckingham: Open University Press 2001).

-- 'Surveillance as social sorting: computer codes and mobile bodies' in David Lyon (ed) *Surveillance as Social Sorting Privacy, risk, and digital discrimination* (Routledge 2003).

-- *Surveillance Studies: An Overview* (Cambridge: Polity Press 2007).

-- 'Surveillance, power, and everyday life' in Chrisanthi Avgerou, Robin Mansell, Danny Quah, and Roger Silverstone (eds) *The Oxford Handbook of Information and Communication Technologies* (Oxford University Press 2009).

-- 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique' (2014) Big Data & Society 1:2 1.

MacAskill E, ‘''Extreme surveillance' becomes UK law with barely a whimper’ *The Guardian* (London, 19 November 2016) <https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper> accessed 11 December 2016.

MacAskill E, Borger J, Hopkins N, Davies N and Ball J, ‘GCHQ taps fibre-optic cables for secret access to world's communications’ *The Guardian* (London, 21 Jun 2013) <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> accessed 5 January 2018.

Machkovech S, ‘Report: Facebook helped advertisers target teens who feel “worthless”’ *Ars Technica* (1 May 2017) <https://arstechnica.com/business/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless/> accessed 2 May 2017.

Maher J, ‘Proportionality analysis after Eweida and Others v. UK: Examining the Connections between Articles 9 and 10 of the ECHR’ (June 2013) <http://ohrh.law.ox.ac.uk/proportionality-analysis-after-eweida-and-others-v-uk-examining-the-connections-between-articles-9-and-10-of-the-echr/> accessed 6 May 2017.

Malloggi F, ‘The Value of Privacy for Social Relationships’ (2017) Social Epistemology Review and Reply Collective 6:2 68.

Mann S, ‘Sousveillance, not just surveillance, in response to terrorism’ (2002) Metal and Flesh 6:1 <http://wearcam.org/metalandflesh.htm> accessed 4 September 2017.

Mann S, Nolan J and Wellman B, ‘Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments’ (2003) Surveillance & Society 1:3 331.

Manokha I, ‘Surveillance, Panopticism, and Self-Discipline in the Digital Age’ (2018) Surveillance and Society 16:2 219.

Mantzaris A, ‘'Totalitarianism', Treason and Containment in Catch-22 (and 1984)’ Comparative American Studies An International Journal 9:3 217

Marshall J, ‘WTF is third-party data?’ (5 February 2014) <https://digiday.com/media/what-is-third-party-data/> accessed 8 April 2017.

Marx G.T, *Undercover: Police Surveillance in America* (University of California Press, Berkeley 1989).

-- ‘What’s New About the “New Surveillance”? Classifying for Change and Continuity’ (2002) Surveillance & Society 1:1: 9.

-- ‘Seeing Hazily, But Not Darkly, Through the Lens: Some Recent Empirical Studies of Surveillance Technologies' (2005) Law and Social Inquiry, 30:2 339.

-- Marx, ‘Soft surveillance: the growth of mandatory volunteerism in collecting personal information – “Hey buddy can you spare a DNA”’ in Torin Monahan (ed), *Surveillance and Security: Technological Politics and Power in Everyday Life*, (London: Routledge 2007).

Martin A.H, 'Home Office admits it's preparing to accept EU ruling on surveillance' *The Register* (London, 21 March 2017) <https://www.theregister.co.uk/AMP/2017/03/21/home_office_admits_its_preparing_to_accept_eu_ruling_on_surveillance/> accessed 21 June 2017.

Martindale, 'UK VPN usage explodes as Digital Economy Bill progresses' (20 December 2016) <https://www.kitguru.net/gaming/security-software/jon-martindale/uk-vpn-usage-explodes-as-digital-economy-bill-progresses/> accessed 11 September 2017.

Marwick A.E, 'The Public Domain: Surveillance in Everyday Life' (2012) Surveillance & Society 9:4 378.

Masnik M, 'Michael Hayden Gleefully Admits: We Kill People Based On Metadata' *Techdirt* (12 May 2014) <https://www.techdirt.com/articles/20140511/06390427191/michael-%20hayden-gleefully-admits-we-kill-people-based-metadata.shtml> accessed 9 April 2017..

Mason A, 'Investment in Network, Facilities, and Equipment by Content and Application Providers' (September 2014), <http://www.analysysmason.com/Research/Content/Reports/Content-application-provider-Internet-infrastructure-Sept2014/Report/> accessed 30 November 2017.

Masterman R, 'Rebalancing the Unbalanced Constitution: Juridification and National Security in the United Kingdom' in Fergal F. Davis and Fiona de Londras (eds), *Critical debates on counter-terrorist judicial review* (Cambridge University Press 2014).

Mataga Z, 'The Right to Freedom of Association Under the European Convention on the Protection of Human Rights and Fundamental Freedoms' (October 2006) <http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan044376.pdf> accessed 9 May 2017.

Mattern F and Floerkemeier C, 'From the internet of computers to the internet of things' in Kai Sachs, Ilia Petrov and Pablo Guerrero (eds) *From Active Data Management to Event-Based Systems and More* (Springer, Berlin, Heidelberg 2010).

-- 'From the Internet of Computers to the Internet of Things' <http://vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf> accessed 25 July 2017.

Matthews A and Tucker C, 'Government Surveillance and Internet Search Behavior' 17 February 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564> accessed 4 May 2017.

Matyszczyk C, 'Judge rules pacemaker data can be used against defendant' (12 July 2017) <https://www.cnet.com/news/judge-rules-pacemaker-data-can-be-used-against-defendant/?ftag=COS-05-10aaa0b&linkId=39705414> accessed 25 August 2017.

Mayera J, Mutchlera P and Mitchella J.C, 'Evaluating the privacy properties of telephone metadata' (2016) PNAS 113:20 5536.

May T, 'Home Secretary: Publication of draft Investigatory Powers Bill' (4 November 2015) <https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill> accessed 3 April 2017.

-- 'Prime Minister Theresa May's speech at the 2018 Munich Security Conference' (17 February 2018) <https://www.gov.uk/government/speeches/pm-speech-at-munich-security-conference-17-february-2018> accessed 9 April 2018.

McCarthy K, 'UK's new Snoopers' Charter just passed an encryption backdoor law by the backdoor' *The Register* (London, 30 November 2016) accessed <http://www.theregister.co.uk/2016/11/30/investigatory_powers_act_backdoors/> 17 January 2017.

McDowell G, 'What Can You Learn From An Email Header (Metadata)?' (13 August 2013) <http://www.makeuseof.com/tag/what-can-you-learn-from-an-email-header-metadata/> accessed 4 April 2017.

McGoogan C, 'Hackers targeting UK energy grid, GCHQ warns' *The Telegraph* (London, 18 July 2017) <http://www.telegraph.co.uk/technology/2017/07/18/hackers-targeting-uk-energy-grid-gchq-warns/> accessed 21 August 2017.

McIntyre T.J, 'Data retention in Ireland: Privacy, policy and proportionality' (2008) Computer Law and Security Report 24:4 326.

-- 'Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective' in Martin Scheinin, Helle Krunke, and Marina Aksenova (eds) *Judges as Guardians of Constitutionalism and Human Rights* (Edward Elgar, 2015).

McKay S, 'Defining Surveillance' (22 January 2016) <https://simonmckay.wordpress.com/2016/01/22/defining-surveillance/> accessed 22 November 2017.

McLean A, 'Data-retention legislation sending Australians into the arms of VPN providers' *ZDNet* (2 June 2017) <http://www.zdnet.com/article/data-retention-legislation-sending-australians-into-the-arms-of-vpn-providers/> accessed 24 June 2017.

McMullan, 'What does the panopticon mean in the age of digital surveillance?' *The Guardian* (London, 23 July 2015) <https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham> accessed 18 December 2016.

Mendola M, 'One Step Further in the 'Surveillance Society': The Case of Predictive Policing' (2016) <http://techandlaw.net/wp-content/uploads/2016/10/One-Step-Further-in-the-Surveillance-Society_The-Case-of-Predictive-Policing.pdf> accessed 24 August 2017.

MI5, 'Bulk Personal Datasets' <https://www.mi5.gov.uk/bulk-data> accessed 31 May 2018.

Michael K and Michael M.G, 'The social and behavioural implications of location-based services' (2011) Journal of Location Based Services 5:3-4 121.

Microsoft, 'Bluetooth Wireless Technology FAQ' (24 July 2012) <http://download.microsoft.com/download/9/c/5/9c5b2167-8017-4bae-9fde-d599bac8184a/Bth_FAQ.docx> accessed 6 December 2017.

Milaj J and Bonnici J.P.M, 'Unwitting subjects of surveillance and the presumption of innocence' (2014) Computer Law and Security Review 30:4 419

Milanovic M, *Extraterritorial Application of Human Rights Treaties Law, Principles, and Policy* (Oxford University Press 2011)

-- 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) Harvard International Law Journal 56, 81.

-- 'UK Investigatory Powers Tribunal Rules that Non-UK Residents Have No Right to Privacy under the ECHR' (18 May 2016) <https://www.ejiltalk.org/uk-investigatory-powers-tribunal-rules-that-non-uk-residents-have-no-right-to-privacy-under-the-echr/> accessed 6 May 2017.

Miller K, 'Why the data retention legislation should be withdrawn' (2 March 2012) <http://www.afr.com/technology/web/why-the-data-retention-legislation-should-be-withdrawn-20150227-13qufg> accessed 31 July 2017.

Mitrou L, 'Communications Data Retention: A Pandora's Box for Rights and Liberties?' in Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis, and Sabrina di Vimercati (ed) *Digital Privacy: Theory, Technologies, and Practices* (Auerbach Publications 2007).

-- 'The impact of communications data retention on fundamental rights and democracy – the case of the EU Data Retention Directive in Kevin D. Haggerty and Minas Samatas (ed) *Surveillance and Democracy* (Routledge and Cavendish 2010).

Molina-Markham A, Shenoy P, Fu K, Cecchet E, and Irwin D, 'Private Memoirs of a Smart Meter' (2010) <http://lass.cs.umass.edu/papers/pdf/buildsys10.pdf> accessed 9 December 2017.

Moody G, 'Google is threatening to throw me off Google+, but won't tell me why' *Ars Technica* (19 December 2016) <http://arstechnica.co.uk/information-technology/2016/12/google-is-threatening-to-throw-me-off-its-g-service-but-wont-tell-me-why/> accessed 21 December 2016

Morariu M, 'How Secure is to Remain Private? On the Controversies of the European Data Retention Directive' Amsterdam Social Science 1:2 46.

Moreham N, 'The right to respect for private life in the European Convention on Human Rights: a re-examination' (2008) EHRLR 1 44.

Mowbray A, 'Creativity of the European Court of Human Rights' (2005) Human Rights Law Review 5:1 57.

-- 'A Study of the Principle of Fair Balance in the Jurisprudence of the European Court of Human Rights' (2010) Human Rights Law Review 10:2 289.

-- 'Contemporary aspects of the promotion of democracy by the European Court of Human Rights' (2014) European Public Law 20:3 469.

Müller-Keezel A, '3 potential holes in WhatsApp's end-to-end encryption' (4 May 2016) <https://venturebeat.com/2016/05/04/3-potential-holes-in-whatsapps-end-to-end-encryption/> accessed 18 August 2017.

Mumford S and Anjum R.L, 'Powers, Non-Consent and Freedom' (2014) Philosophy and Phenomenological Research 91:1 136.

Mundy O, 'Stasi networks and Facebook Social Graph' (28 May 2017) <http://owenmundy.com/blog/2017/05/stasi-facebook-big-data-daad-day-17-stasi-networks-and-facebook-social-graph/> accessed 13 October 2017.

Munir A.B and Yasin S.H.M, 'Retention of communications data: A bumpy road ahead' (2004) The John Marshall Journal of Computer & Information Law 22:4 731.

Murphy T and Cuinn G.O, 'Works in Progress: New Technologies and the European Court of Human Rights' (2010) HRLR 10:4 60.1

Murray A.D, 'Data transfers between the EU and UK post Brexit?' (2017) International Data Privacy Law 7:3 149.

National Institute of Open Schooling 'Internet Applications and Services' <http://oer.nios.ac.in/wiki/index.php/INTERNET_APPLICATION_AND_SERVICES> accessed 10 April 2017.

Naughton J, 'Edward Snowden: public indifference is the real enemy in the NSA affair' *The Guardian* (London, 20 October 2013) <https://www.theguardian.com/world/2013/oct/20/public-indifference-nsa-snowden-affair> accessed 10 December 2016.

-- 'Death by drone strike, dished out by algorithm' *The Guardian* (London, 21 February 2016) <https://www.theguardian.com/commentisfree/2016/feb/21/death-from-above-nia-csa-skynet-algorithm-drones-pakistan> accessed 3 June 2018.

-- 'Good luck in making Google reveal its algorithm' *The Guardian* (London, 13 November 2016) <https://www.theguardian.com/commentisfree/2016/nov/13/good-luck-in-making-google-reveal-its-algorithm> accessed 9 December 2016.

Negraa R *et al*, 'Wireless Body Area Networks: Applications and technologies' (2016) Procedia Computer Science 83 1274.

Nehf J.P, 'Recognising the Societal Value in Information Privacy' (2003) Wash. L. Rev. 78 1.

Netflow Auditor <http://www.netflowauditor.com/> accessed 23 November 2017

-- <http://netflowauditor.com/details.php> accessed 23 November 2017.

Neuberger, '"What's in a name?" - Privacy and anonymous speech on the Internet' (30 September 2014) <https://www.supremecourt.uk/docs/speech-140930.pdf> accessed 29 April 2017.

Neupane A, Rahman L and Saxena N, 'PEEP: Passively Eavesdropping Private Input via Brainwave Signals' (2017) <https://info.cs.uab.edu/saxena/docs/nrs-fc17.pdf> accessed 5 September 2017.

Newell B.C, 'The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe' (2014) I/S A Journal of Law and Policy for the Information Society 10:2 481.

Ng A and Musil S, 'Equifax data breach may affect nearly half the US population' *CNet* (7 September 2017) <https://www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population/> accessed 10 October 2017.

Ng V and Murray D, 'Extraterritorial Human Rights Obligations in the Context of State Surveillance Activities?' (2 August 2016) <https://www.hrbdt.ac.uk/extraterritorial-human-rights-obligations-in-the-context-of-state-surveillance-activities/> accessed 6 May 2017.

Nieuwenhuis A, 'The Concept of Pluralism in the Case-Law of the European Court of Human Rights' (2007) European Constitutional Law Review 3: 367.

-- 'Review of Privacy vs Security' (2015) Utrecht Journal of International and European Law 31:80 137.

Nowak M, *UN Covenant on Civil and Political Rights. CCPR Commentary* (2nd rev. ed.). (Kehl am Rhein: Engel, 2005).

Nyst C, 'At last, the data giants have been humbled' *The Guardian* (London, 7 October 2015) <http://www.theguardian.com/commentisfree/2015/oct/07/data-giants-internet-legal-facebook-google> accessed 31 May 2018.

Obar J.A and Oeldorf-Hirsch A, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (24 August 2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465> accessed 9 December 2016.

O'Cleirigh F, 'Bill Binney, the 'original' NSA whistleblower, on Snowden, 9/11 and illegal surveillance' *Computers Weekly* (April 2015) <http://www.computerweekly.com/feature/Interview-the-original-NSA-whistleblower> accessed 7 March 2017.

O'Connell R, 'Cinderella comes to the Ball: Art 14 and the right to non-discrimination in the ECHR' (2009) Legal Studies 29:2 221.

O'Brien D, 'Data Privacy Means Data Security (and not Data Retention)' (27 January 2014) <https://www.eff.org/deeplinks/2014/01/data-privacy-means-data-security-and-not-data-retention> accessed 21 August 2017.

Odinot G, de Jong D, Bokhorst R.J and de Poot C.J, 'The Dutch implementation of the Data Retention Directive' (2014) <https://www.wodc.nl/binaries/ob310a-full-text_tcm28-78190.pdf> accessed 9 August 2017,

Ogura T, 'Electronic government and surveillance-oriented society' in David Lyon (ed) *Theorizing surveillance: The Panopticon and Beyond* (Portland, OR: Willan 2006).

Office for National Statistics. 'Internet users in the UK 2017' (19 May 2017) <https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2017> accessed 3 January 2018.

Official Lunix Bluetooth stack, <http://www.bluez.org/> accessed 6 December 2017.

Ojanen T, 'Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance' (2014) European Constitutional Law Review 10: 528.

Omtzigt P, Committee on Legal Affairs and Human Rights, 'Mass surveillance' (26 January 2015) <http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10b7a2> accessed 8 May 2017.

Olander T, 'In Denmark, Online Tracking of Citizens is an Unwieldy Failure' (22 May 2013) <http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy> accessed 10 August 2017.

Olivi G, 'Europe: Artificial Intelligence, what can we learn from the GDPR?' (7 February 2017) <https://blogs.dlapiper.com/privacymatters/europe-artificial-intelligence-what-can-we-learn-from-the-gdpr/> accessed 15 March 2018.

O'Neil C, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Penguin Books 2017).

-- 'The era of blind faith in big data must end' (April 2017) <https://www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end#t-786714> accessed 17 October 2017.

Oostveen M, 'Identifiability and the applicability of data protection to big data' (2016) International Data Privacy Law 0:0 1.

Opening Remarks by Ms. Navi Pillay United Nations High Commissioner for Human Rights to the Expert Seminar: The right to privacy in the digital age, (24 February 2014), Room XXI, Palais des Nations, Geneva, <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=E> accessed 14 February 2017.

Open Rights Group, 'Briefing to MPs on Data Retention Legislation' (9 July 2014) <https://www.openrightsgroup.org/ourwork/reports/briefing-to-mps-on-data-retention-legislation> accessed 15 June 2016.

-- 'Cashing in on your mobile? How phone companies are exploiting their customers' data' (4 March 2016) <https://regmedia.co.uk/2016/04/04/cashinginonyourmobile.pdf> accessed 17 April 2017.

-- 'THE INVESTIGATORY POWERS BILL'S IMPACT WILL REACH BEYOND THE UK' (2016) <https://www.openrightsgroup.org/press/releases/2016/ipb-will-reach-beyond-the-uk> accessed 21 November 2016.

-- 'Internet Connection Records' <https://www.openrightsgroup.org/assets/files/pdfs/submissions/ORGSTCsubmissionIPB.pdf > accessed 7 August 2017.

-- 'Digital Surveillance' <https://www.openrightsgroup.org/assets/files/pdfs/reports/digital-surveillance.pdf> accessed 12 August 2017.

Open Society Initiative, 'Equality under Pressure: The Impact of Ethnic Profiling' (2013) <https://www.opensocietyfoundations.org/sites/default/files/equality-under-pressure-the-impact-of-ethnic-profiling-netherlands-20131128_1.pdf> accessed 19 October 2017.

Opinion 7/2000 of the Article 29 Working Party concerning the processing of personal data and the protection of privacy in the electronic communications sector (12 July 2000) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp36_en.pdf> accessed 30 November 2017.

Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime' (22 March 2001) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp41_en.pdf> accessed 23 May 2017.

Opinion 9/2004 of Article 29 Data Protection Working Party, (9 November 2004) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp99_en.pdf> accessed 22 November 2017.

Opinion 8/2016 'EDPS Opinion on coherent enforcement of fundamental rights in the age of big data' (23 September 2016) <https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf> accessed 13 November 2017.

Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)], <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp99_en.pdf> accessed 17 April 2017.

Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive

(Directive 2006/24/EC) (2011) <http://www.statewatch.org/news/2011/may/edps-opinion-eu-mand-ret-opinion.pdf> accessed 5 June 2017.

-- on net neutrality, traffic management and the protection of privacy and personal data, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012XX0208(01)> accessed 17 April 2017.

Opinion of the Legal Service, 'Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism' (5 April 2005) <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207688%202005%20INIT> accessed 25 May 2017.

Oracle8i, 'Data Warehousing Guide'<http://docs.oracle.com/cd/A87860_01/doc/server.817/a76994/toc.htm> accessed 4 December 2017.

Orwell G, *Nineteen Eighty-Four* (Penguin Classics 2013).

Osborne C, 'How hackers can hijack brainwaves to capture your passwords' *ZDNet* (8 May 2017) <http://www.zdnet.com/google-amp/article/how-hackers-use-brainwaves-to-capture-your-passwords/?utm_content=buffer5b8d1&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer> accessed 5 September 2017.

Oxford English Dictionary, 'big data' <https://en.oxforddictionaries.com/definition/big_data> accessed 3 June 2018.

Oxford Living Dictionaries <https://en.oxforddictionaries.com/definition/surveillance> accessed 16 November 2017.

PageFair, 'The state of the blocked web 2017 Global Adblock Report' (2017) <https://pagefair.com/downloads/2017/01/PageFair-2017-Adblock-Report.pdf> accessed 20 September 2017.

Pannick D, 'David Pannick: Safeguards provide a fair balance on surveillance powers' *The Times* (London, November 12 2015) <http://www.thetimes.co.uk/tto/law/article4611174.ece> accessed 18 July 2017.

Pariser E, *The Filter Bubble* (Penguin Books 2012.

Parsons C, 'Privacy Tech-Know Blog: Uniquely You: The identifiers on our phones that are used to track us' (8 December 2016) <http://blog.priv.gc.ca/index.php/2016/12/08/privacy-tech-know-blog-uniquely-you-the-identifiers-on-our-phones-that-are-used-to-track-us/> accessed 24 April 2017.

-- 'IMSI Catchers in Canada Resources' <https://www.christopher-parsons.com/writings/imsi-catchers-resource-page/> accessed 11 April 2017.

Pasquale F, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press, Cambridge, MA, 2015.

Patron T, 'The Investigation of Packets' (13 November 2015) <https://babyis60.wordpress.com/2015/11/13/the-investigation-of-packets/> accessed 9 August 2017.

Payton M, 'Japan's top court has approved blanket surveillance of the country's Muslims' *The Independent* (London, 29 June 2016) <http://www.independent.co.uk/news/world/asia/muslims-japan-government-surveillance-top-court-green-lit-islamaphobia-a7109761.html> accessed 2 November 2016.

Pearce D, Campbell E and Harding D, *Australian Law Schools: A Discipline Assessment for the Commonwealth Tertiary Education Commission 1987*.

Pedersen A.M, Udsen H and Jakobsen S.S, 'Data retention in Europe—the *Tele 2* case and beyond' (2018) International Data Privacy Law 0:0.

Peers S, 'The data retention judgment: The CJEU prohibits mass surveillance' (8 April 2014) <https://eulawanalysis.blogspot.co.uk/2014/04/the-data-retention-judgment-cjeu.html> accessed 13 June 2017.

PEN America, 'Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor' (12 November 2013) <https://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf> accessed 16 April 2018.

Penney J, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) Berkeley Technology Law Journal 31:1 117 <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2104&context=btlj> accessed 5 May 2017.

-- 'Internet surveillance, regulation, and chilling effects online: a comparative case study' (2017) Internet Policy Review 6:2.

-- 'Whose Speech Is Chilled by Surveillance?' (7 July 2017) <http://www.slate.com/articles/technology/future_tense/2017/07/women_young_people_experience_the_chilling_effects_of_surveillance_at_higher.html> accessed 17 August 2017.

Pentland A, 'Society's Nervous System: Building Effective Government, Energy, and Public Health Systems' (2012) Computer 45:1 31.

Pérez M.F, 'Tinder and me: My life, my business' (4 October 2017) <https://edri.org/tinder-my-life-my-business/> accessed 1 November 2017.

Perry T.S, 'A Sleeping Alexa Can Listen for More Than Just Her Name' (9 February 2018) <https://spectrum.ieee.org/view-from-the-valley/consumer-electronics/gadgets/beyond-the-super-bowl-a-sleeping-alexa-can-listen-for-more-than-just-her-name.amp.html?__twitter_impression=true> accessed 17 June 2018.

Peterson A, 'eBay asks 145 million users to change passwords after data breach' *The Washington Post* (Washington, D.C, 21 May 2014) <https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/> accessed 10 October 2017.

-- 'Why Edward Snowden thinks you should use an ad blocker' *The Washington Post* (Washington, D.C, 13 November 2015) <https://www.washingtonpost.com/news/the-switch/wp/2015/11/13/why-edward-snowden-thinks-you-should-use-an-ad-blocker/> accessed 20 September 2017.

Pettit P, *Republicanism* (Oxford: OUP, 1997).

Pexip, 'Streaming a conference over YouTube' <https://docs.pexip.com/admin/streaming_youtube.htm> accessed 10 May 2017.

Pimenidis L and Kosta E, 'The impact of the retention of traffic and location data on the internet user' (2008) DuD Datenschutz und Datensicherheit 32:2 92.

Press Association, 'Vodafone customers' bank details 'accessed in hack', company says' *The Guardian* (London, 31 October 2015) <https://www.theguardian.com/business/2015/oct/31/vodafone-customers-bank-details-accessed-in-hack-company-says> accessed 21 August 2017.

Privacy International, 'Memorandum of Laws concerning the Legality of Data Retention with regard to the Rights guaranteed by the European Convention on Human Rights' (10 October 2003) <http://www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf> accessed 25 May 2017.

-- 'The database of you: Internet Connection Records will allow the UK Government to document everything we do online' <https://www.privacyinternational.org/node/1011> accessed 10 October 2017.

-- 'Location Monitoring' <https://www.privacyinternational.org/node/74> accessed 11 April 2017.

-- 'UK Investigatory Powers Bill will require tech companies to notify the Government of new products and services in advance of their launch' (16 April 2016) <https://www.privacyinternational.org/node/829> accessed 26 November 2016.

-- 'What UK politicians can, and must, do about the Cambridge Analytica/Facebook scandal' (23 March 2018) <https://ceasefiremagazine.co.uk/uk-politicians-can-must-cambridge-analytica-facebook-scandal/> accessed 16 April 2018.

-- 'Press release: UK intelligence agency admits unlawfully spying on Privacy International' (25 September 2018) <https://privacyinternational.org/press-release/2283/press-release-uk-intelligence-agency-admits-unlawfully-spying-privacy> accessed 11 October 2018.

Portela I.M and Cruz-Cunha M.M, 'What About the Balance Between Law Enforcement and Data Protection?' in Irene Maria Portela and Maria Manuela Cruz-Cunha (eds) *Information*

Communication Technology Law, Protection and Access Rights: Global Approaches and Issues, (IGI Global 2010).

Porup J.M, 'The Internet of Things is a surveillance nightmare' (20 March 2016) <http://kernelmag.dailydot.com/issue-sections/staff-editorials/16196/internet-of-things-surveillance-nightmare/> accessed 3 September 2017.

Posetti J, 'Protecting Journalism Sources in the Digital Age' (2017) <http://unesdoc.unesco.org/images/0024/002480/248054E.pdf> accessed 13 November 2017,

Posner R.A, 'Our Domestic Intelligence Crisis' *The Washington Post* (Washington, D.C, 21 December 2005) <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html> accessed 3 January 2018.

Poster M, *The mode of information* (Cambridge: Polity 1990).

Poullet Y,'The Fight against Crime and/or the Protection of Privacy: A Thorny Debate!' (2004) International Review of Law Computers and Technology 18:2 251.

Pounder C, 'Nine principles for assessing whether privacy is protected in a surveillance society' (2008) Identity Journal Limited 1:1 1.

-- 'Information Commissioner should enforce Article 8 privacy rights' (20 April 2010) <http://amberhawk.typepad.com/amberhawk/2010/04/information-commissioner-should-enforce-article-8-privacy-rights.html> accessed 22 August 2017.

-- 'Letter to Dr Chris Pounder from the Ministry of Justice' (5 May 2011) <amberhawk.typepad.com/files/uk-deficiency-details_may-2011.pdf> accessed 9 April 2018.

-- 'Information Commissioner's enforcement proceedings links Article 8 to unlawful processing' (8 November 2012) <http://amberhawk.typepad.com/amberhawk/2012/11/information-commissioners-enforcement-proceedings-links-article-8-to-unlawful-processing.html> accessed 22 August 2017.

-- 'Question answered: "Why does the European Commission think the UK's Data Protection Act is a deficient implementation of Directive 95/46/EC?"' (6 February 2013) <amberhawk.typepad.com/amberhawk/2013/02/question-answered-why-does-the-european-commission-think-the-uks-data-protection-act-is-a-deficient-implementation-of.html> accessed 9 April 2018.

-- 'Why the UK is unlikely to get an adequacy determination post Brexit' (9 January 2017) <http://amberhawk.typepad.com/amberhawk/2017/01/why-the-uk-is-unlikely-to-get-an-adequacy-determination-post-brexit.html> last accessed 9 April 2018.

-- 'Is the NHS ransomware incident a reportable data loss?' (14 May 2017) <http://amberhawk.typepad.com/amberhawk/> accessed 19 May 2017.

Press Release: The Minister of Justice repeals the rules for session logging (2 June 2014) <http://justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2014/justitsministeren-oph%C3%A6ver-reglerne-om-sessionslogning> accessed 10 August 2017.

Quinton, B, 'They'll make an ISP out of you' (1999) Telephony 237:22 88.

Radar, 'Investigatory Powers Act' (5 January 2017) <https://united-kingdom.taylorwessing.com/en/insights/radar-december-2016-data-protection> accessed 5 December 2017.

Rainie L and Anderson J, 'Code-Dependent: Pros and Cons of the Algorithm Age' (8 February 2017) <http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/02/08181534/PI_2017.02.08_Algorithms_FINAL.pdf> accessed 19 October 2017.

Ranger S, 'The undercover war on your internet secrets: How online surveillance cracked our trust in the web' *TechRepublic* (Louisville, Kentucky, 12 June 2016) <https://web.archive.org/web/20160612190952/http://www.techrepublic.com/article/the-undercover-war-on-your-internet-secrets-how-online-surveillance-cracked-our-trust-in-the-web/> accessed 17 November 2016.

Rauhofer J, 'Just Because You're Paranoid, Doesn't Mean They're Not After You: Legislative Developments in Relation to the Retention of Communications Data' (2006) SCRIPTed 3 322.

Rauhofer J and Síthigh D.M, 'The Data Retention Directive Never Existed' (2014) SCRIPTed 11:1 118.

Recommendation CM/Rec(2014)6.

Recommendation Rec(2005)10 of the Committee of Ministers to member states on "special investigation techniques" in relation to serious crimes including acts of terrorism, 20 April 2005.

Reed A and Kranch M, 'Identifying HTTPS-Protected Netflix Videos in Real-Time' (March 2017) <http://www.mjkranch.com/docs/CODASPY17_Kranch_Reed_IdentifyingHTTPSNetflix.pdf> accessed 9 April 2017.

Reid A.S, 'Is society smart enough to deal with smart cards?' (2007) Computer Law Security Report 23:1 53.

-- 'The European Court of Justice case of Breyer' (2017) Journal of Information Rights, Policy and Practice 2:1 1.

Reid A.S and Ryder N, 'For Whose Eyes Only? A Critique of the United Kingdom's Regulation of Investigatory Powers Act 2000' (2001) Information & Communications Technology Law 10:2 179.

Regan P.M, *Legislating Privacy, Technology, Social Values and Public Policy* (The University of North Carolina Press 1995).

Regulation of Investigatory Powers Bill Deb 16 March 2000.

Regulation of Investigatory Powers Bill Deb 12 Jun 2000, Column 1421.

Report of the Interception of Communications Commissioner, 'Annual Report for 2015' (8 September 2016) <http://iocco-uk.info/docs/56850%20HC%20255%20ICCO%20Web%20only.pdf> accessed 18 April 2017.

Report of the Interception of Communications Commissioner Annual Report for 2015 (HC 255 8 September 2016).

Reporters Without Borders, 'A worrying trend' (2017) <https://rsf.org/en/united-kingdom> accessed 13 November 2017.

Report of the Interception of Communications Commissioner Annual Report for 2015 (HC 255 8 September 2016).

Retention of Communications Data under Part 11: Anti-terrorism, Crime and Security Act 2001 Voluntary Code of Practice <http://www.opsi.gov.uk/si/si2003/draft/5b.pdf> accessed 17 April 2017.

RevK's Rants 'What is an "Internet Connection Record"?' (14 November 2016) <http://www.revk.uk/2015/11/what-is-internet-connection-record.html> accessed 9 August 2017.

Richmond S, Rees G and Edwards S.J.L, *I Know What You're Thinking: Brain imaging and mental privacy* (Oxford University Press 2012).

Ringland K, 'The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model' (2009) SHIDLER J. L. COM. & TECH 5:3.

Roagna I, 'Protecting the right to respect for private and family life under the European Convention on Human Rights' (2012) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806f1554> accessed 6 April 2017.

Roberts A, 'Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications' (2015) MLR 78:3 522.

Roberts H and Palfrey J, 'The EU Data Retention Directive in an Era of Internet Surveillance' in Ronald J. Deibert and others (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (MIT Press 2010).

Roessler B and Mokrosinska D 'Introduction' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy Interdisciplinary Perspectives* (Cambridge University Press 2015).

Rhoen M, 'Beyond consent: improving data protection through consumer protection law' (2016) Internet Policy Review 5:1 1.

Rogerson L, 'How a smart meter could save your life' *The Spectator* (18 July 2018) <https://health.spectator.co.uk/how-a-smart-meter-could-save-your-life/?_lrsc=dbc7fdf0-368e-4711-9bae-da8fa3fa3d4b&_lrsc=cf7b4f02-2490-43e2-98c6-d075e421c98c> accessed 30 July 2018.

Roskies A.L, 'Mind Reading, Lie Detection, and Privacy' in Jens Clausen and Neil Levy (ed), *Handbook of Neuroethics* (Springer Netherlands 2015).

Roudik P, 'Russia: New Electronic Surveillance Rules' (18 July 2016) <https://www.loc.gov/law/foreign-news/article/russia-new-electronic-surveillance-rules/> accessed 12 April 2018.

Rouse M, 'MAC address (Media Access Control address)' *TechTarget* <http://searchnetworking.techtarget.com/definition/MAC-address> accessed 10 April 2017.

-- 'next-generation firewall (NGFW)' *TechTarget* <http://searchsecurity.techtarget.com/definition/next-generation-firewall-NGFW> accessed 6 December 2017.

-- 'Deep packet inspection (DPI)' *TechTarget* (November 2007) <http://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPI> accessed 6 December 2017

Rouvroy A, '"Of Data and Men" - Fundamental rights and freedoms in a world of Big Data' (11 January 2016) <https://rm.coe.int/16806a6020> accessed 6 November 2017.

Rubinstein I.S, 'Big Data: The End of Privacy or a New Beginning?' (2013) International Data Privacy Law 3:2 74.

Ruiz J, 'EU Court slams UK data retention surveillance regime' (21 December 2016) <https://www.openrightsgroup.org/blog/2016/eu-court-slams-uk-data-retention-surveillance-regime> accessed 21 June 2017.

RUSI, 'A Democratic Licence to Operate' (15 July 2015) <https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf> accessed 3 April 2017.

Rutzen D and Zenn J, 'Association and Assembly in the Digital Age' (2011) The International Journal of Not-for-Profit Law 13:4.

Ryan M.H, 'Is government access to your communications data lawful? The decision of the Divisional Court in Davis v Home Secretary' U.L.R. [2015] 20:5

Ryberg J, 'Neuroscience, Mind Reading and Mental Privacy' (2017) Res Publica 23:2 197.

Sabel R, 'How NetFlow Solves for Mandatory Data Retention Compliance' (8 August 2016) <http://blog.netflowauditor.com/how-netflow-solves-for-data-retention-compliance> accessed 16 December 2016.

Saiban J and Sykes J, 'UK ANTI-TERRORISM ACT 2001 & ISP'S: A CYBER CHECK-POINT CHARLIE?' (2002) Computer Law & Security Review 18:5 338.

Sapharishi M, 'The New Eyes of Surveillance: Artificial Intelligence and Humanizing Technology' *Wired* (San Francisco, California, August 2014) <https://www.wired.com/insights/2014/08/the-new-eyes-of-surveillance-artificial-intelligence-and-humanizing-technology/> accessed 18 November 2017.

Saul, 'The European Court of Human Rights' Margin of Appreciation and the Processes of National Parliaments' (2015) Human Rights Law Review 15 745.

Scassa T, 'Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy' (2009) Canadian Journal of Law and Technology 9:2 193.

SC Deb (F) 28 March 2000, col 252.

Schaeffer A, 'Linking Marleasing and s. 3(1) of the Human Rights Act 1998' (2005) Judicial Review 10:1.

Scheiber N, 'How Uber Uses Psychological Tricks to Push Its Drivers' Buttons' *New York Times* (New York City, 2 April 2017) <https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html?smid=tw-share&_r=0> accessed 25 November 2017.

Scheinin M, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism' A/HRC/13/37 (28 December 2009) <http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf> accessed 14 May 2017

Schermer B.W, 'Surveillance and Privacy in the Ubiquitous Network Society' (2009) 1:4 <http://amsterdamlawforum.org/article/view/95/169> accessed 22 November 2017.

Schep T, 'Data Leads to Social Cooling' <https://www.socialcooling.com/> accessed 20 September 2017.

Schneier B, 'Security vs. Privacy' (29 January 2008), <https://www.schneier.com/blog/archives/2008/01/security_vs_pri.html> accessed 7 March 2017.

-- *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W.W. Norton 2016).

Schwartz P.M, 'Privacy and Democracy in Cyberspace' (1999) Vand. L. Rev. 52 1607.

Science and Technology Committee, *Investigatory Powers Bill: technology issues (third report)* (2015–16, HC 573).

Secretary of State for the Home Department, *Rights Brought Home* (White Paper, Cm 3782 (1997)).
Shen F.X, 'Neuroscience, Mental Privacy, and the Law' (2013) Harvard Journal of Law & Public Policy 36:2 653.

Sheridan C, 'Foucault, Power and the Modern Panopticon' (2016) Senior Theses, Trinity College, Hartford, CT 2016. Trinity College Digital Repository <http://digitalrepository.trincoll.edu/theses/548> accessed 25 November 2016.

Shields P, 'Electronic Networks, Enhanced State Surveillance and the Ironies of Control' (2006) Journal of Creative Communications 1:1.

Sidhu D.S, 'The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim Americans' (2007) 7 U. Md. L.J. Race Relig. Gender & Class 375 7:2: <http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1134&context=rrgc> accessed 12 May 2017.

Simonite T, 'Using Brainwaves to Guess Passwords' *MIT Technology Review* (Cambridge, Massachusetts, 5 May 2017) <https://www.technologyreview.com/s/604293/using-brainwaves-to-guess-passwords/?set=604330> accessed 5 September 2017.

Skinner Q and Marshall R, 'Liberty, Liberalism and Surveillance: a historic overview' *openDemocracy* (26 July 2013) <https://www.opendemocracy.net/ourkingdom/quentin-skinner-richard-marshall/liberty-liberalism-and-surveillance-historic-overview> accessed 9 November 2017.

Smith C, 'iOS 9.3 will tell you if your employer is tracking your iPhone' (2 March 2016) <http://bgr.com/2016/03/02/work-iphone-privacy-ios-9-3/> accessed 21 November 2017.

Small J, 'Structure and Substance: Developing a Practical and Effective Prohibition on Discrimination under the European Convention on Human Rights' (2003) International Journal of Discrimination and the Law 6 45.

Smith G, *Internet Law and Regulation* (Sweet and Maxwell 4th edn 2007).

-- 'Mandatory communications data retention lives on in the UK - or does it?' (21 August 2014) <http://uk.practicallaw.com/8-577-6488> accessed 4 December 2017.

-- 'From Oversight to Insight - Hidden Surveillance Law Interpretations' (9 November 2015) <http://cyberleagle.blogspot.co.uk/2015/11/from-oversight-to-insight-hidden.html> accessed 3 December 2017.

-- 'Never mind Internet Connection Records, what about Relevant Communications Data?' (29 November 2015) <http://www.cyberleagle.com/2015/11/never-mind-internet-connection-records.html> accessed 8 April 2017.

-- 'The draft Investigatory Powers Bill - start all over again?' (16 February 2016) <http://www.cyberleagle.com/2016/02/the-draft-investigatory-powers-bill.html> accessed 4 December 2017.

-- 'Relevant Communications Data revisited' (15 March 2016) <http://www.cyberleagle.com/2016/03/relevant-communications-data-revisited.html> accessed 9 April 2017.

-- 'Future-proofing the Investigatory Powers Bill' (15 April 2016) <http://www.cyberleagle.com/2016/04/> accessed 5 March 2018.

-- 'Data retention - the Advocate General opines' (19 July 2016) <http://www.cyberleagle.com/2016/07/data-retention-advocate-general-opines.html> accessed 5 January 2018.

-- 'The UK Investigatory Powers Act 2016 – what it will mean for your business' (29 November 2016) <https://www.twobirds.com/en/news/articles/2016/uk/what-the-investigatory-powers-bill-would-mean-for-your-business> accessed 5 December 2017.

-- 'Illuminating the Investigatory Powers Act' (22 February 2018) <https://www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html> accessed 3 June 2018.

Sobey J, 'Legal professional privilege under fire' <http://www.stokoepartnership.com/wp-content/uploads/2016/06/Jessica-Sobey-Legal-Professional-Privilege-Under-Fire-CLJ-Vol.-180.pdf > accessed 17 May 2017.

Soldatov D.I, 'Data Retention under the 2016 "Yarovaya Law" in Russia: Disrupting the European Status Quo?' (17 March 2017) <https://www.filodiritto.com/articoli/pdf/2017/03/data-retention-under-the-2016-yarovaya-law-in-russia-disrupting-the-european-status-quo.html?_id8=3> accessed 12 April 2018.

Solon O, 'Facebook has 60 people working on how to read your mind' *The Guardian* (London, 19 April 2017) <https://www.theguardian.com/technology/2017/apr/19/facebook-mind-reading-technology-f8> accessed 24 April 2017.

-- 'Credit firm Equifax says 143m Americans' social security numbers exposed in hack' *The Guardian* (London, 8 September 2017) <https://www.theguardian.com/us-news/2017/sep/07/equifax-credit-breach-hack-social-security> accessed 8 September 2017.

Solove D, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) Standford Law Review 53 1393.

-- 'Reconstructing Electronic Surveillance Law' (2004) 72 The George Washington Law Review 1701.

-- *The Digital Person Technology and Privacy in the Information Age* (NYU Press 2006).

-- ‘’I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy’ (2007) San Diego Law Review 44 745.

-- *Understanding Privacy* (Harvard University Press 2009).

-- *Nothing to Hide. The False Trade off between Privacy and Security* (Yale University Press 2011).

Soltani A, (10 April 2018) <https://twitter.com/ashk4n/status/983726143650975749> accessed 16 April 2018.

Sorell T, ‘Preventive policing, surveillance, and European counter-terrorism’ (2011), Criminal Justice Ethics 30:1.

Speaight A, ‘Anthony Speaight QC: Charter reach extended, national security hampered, EU competence exceeded’ (11 January 2017) <https://judicialpowerproject.org.uk/anthony-speaight-qc-tele2-sverige-charter-reach-extended-national-security-hampered-eu-competence-exceeded/> accessed 22 June 2017.

-- ‘Data Retention, National Security and the ECJ: The Continuing Saga’ (6 February 2018) <https://judicialpowerproject.org.uk/anthony-speaight-data-retention-national-security-and-the-ecj-the-continuing-saga/> accessed 19 February 2018.

Splunk, ‘Make Machine Data Accessible, Usable and Valuable to Everyone’ <https://www.splunk.com/pdfs/company-overview.pdf> accessed 11 October 2017.

Stalla-Bourdillon S, ‘Online monitoring, filtering, blocking….What is the difference? Where to draw the line?’ (2013) Computer law & security review 29:6 702.

-- ‘What the hell are these metadata? ….Are communications data, traffic data and metadata all the same thing?’ (30 October 2014) <https://peepbeep.wordpress.com/2014/10/30/what-the-hell-are-these-metadata-are-communications-data-traffic-data-and-metadata-all-the-same-thing/> accessed 17 April 2017.

-- ‘The Davis judgement: does Article 8 of the European Charter go beyond Article 8 of the ECHR?’ (25 July 2015) <https://inforrm.wordpress.com/2015/07/25/the-davis-judgement-does-article-8-of-the-european-charter-go-beyond-article-8-of-the-echr-sophie-stall-bourdillon/> accessed 22 August 2017.

Stalla-Bourdillon S, Papadaki E and Chown T, ‘Metadata, Traffic Data, Communications Data, Service Use Information… What Is the Difference? Does the Difference Matter? An Interdisciplinary View from the UK’ in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move* (Springer 2016),

Statement of the European Data Protection Commissioners, (11 September 2002) <http://www.fipr.org/press/020911DataCommissioners.html> accessed 23 May 2017.

Statewatch, ‘Data or data protection in the EU?’ <http://www.statewatch.org/news/2001/sep/dataprot.pdf> accessed 23 May 2017.

-- ‘European Parliament and EU governments on a collision course over the retention of data (telecommunications surveillance)’ <http://www.statewatch.org/news/2001/nov/15eudata.htm> accessed 23 May 2017.

-- ‘EU: Final decision on surveillance of communications European Commission sells-out, European Parliament vote due in May, January-February 2002, vol 12 no 1’ <http://www.statewatch.org/news/2002/may/05Asurv.htm> accessed 23 May 2017.

-- ‘European Parliament caves in on data retention’ (30 May 2002) <http://www.statewatch.org/news/2002/may/10epcavein.htm> accessed 23 May 2017.

-- ‘The vote in the European Parliament to accept data retention and surveillance by the law enforcement agencies: an analysis’ <http://www.statewatch.org/news/2002/may/15epvote.htm> accessed 23 May 2017.

-- ‘Coalition asks European Parliament to vote against data retention’ ‘(23 May 2002) <http://www.statewatch.org/news/2002/may/09coalition.htm> accessed 23 May 2017.

-- ‘EU: Final decision on surveillance of communications European Commission sells-'out, European Parliament vote due in May’ (January-February 2002) vol 12 no 1, <http://www.statewatch.org/news/2002/may/05Asurv.htm> accessed 25 May 2017.

-- ‘Surveillance of communications: data retention to be “compulsory” for 12-24months’ (2002) < http://www.statewatch.org/news/2002/aug/analy11.pdf> accessed 25 May 2017.

-- ‘Surveillance of communications EU: data retention to be "compulsory" for 12-24 months-draft Framework Decision leaked to Statewatch’ (23 August 2002) <http://www.statewatch.org/news/2002/aug/05datafd1.htm> accessed 25 May 2017.

-- ‘Majority of governments introducing data retention of communications’ <http://www.statewatch.org/news/2003/jan/12eudatret.htm> accessed 23 May 2017.

-- ‘EU/Surveillance of telecommunications: Data retention comes to roost - telephone and internet privacy to be abolished’ (2004) <http://www.statewatch.org/news/2004/apr/21dataretention.htm> accessed 25 May 2017.

Steering Committee on Media and Information Society (CDMSI) (16 April 2014) <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c6f85#P118_25200> accessed 6 April 2017.

Stewart H, ‘May calls on internet firms to remove extremist content within two hours’ *The Guardian* (London, 20 September 2017) <https://www.theguardian.com/uk-news/2017/sep/19/theresa-may-will-tell-internet-firms-to-tackle-extremist-content> accessed 3 December 2017.

Stewart W, ‘Living Internet, How the Internet Works’ <http://www.livinginternet.com/i/iw.htm> accessed 30 November 2017.

Stoeva E, ‘The Data Retention Directive and the right to privacy’ (2014) ERA Forum 15:4 575.

Stoycheff E, 'Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring' (2016) Journalism & Mass Communication Quarterly 93:2 296.

Stych A, 'Social media reunites families after Harvey' (30 August 2017) <https://www.bizjournals.com/bizwomen/news/latest-news/2017/08/social-media-reunites-families-after-harvey.html?page=all> accessed 6 June 2018.

Sulleyman A, 'Snooper's Charter: Majority of Public Unaware of Government Online Surveillance' (22 May 2017) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-investigatory-powers-bill-government-online-surveillance-majority-uk-unaware-a7749851.html> accessed 3 January 2018.

-- Sulleyman, 'Facebook could farm users' thoughts with Mind-Reading technology to sell adverts' *The Independent* (London, 25 May 2017) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-mind-reading-technology-thoughts-sell-adverts-social-media-accounts-a7755136.html> accessed 4 September 2017.

Sullivan J, 'Uncovering the data panopticon: The urgent need for critical scholarship in an era of corporate and government surveillance' (2013) The Political Economy of Communication 1:2.

Summers T, 'Facebook is killing democracy with its personality profiling data' *The Conversation* (Melbourne, 21 March 2018) <https://theconversation.com/facebook-is-killing-democracy-with-its-personality-profiling-data-93611> accessed 3 June 2018.

Suzor N, Pappalardo K and McIntosh N, 'The passage of Australia's data retention regime: national security, human rights, and media scrutiny' (2017) Internet Policy Review 6:1 1.

Sweeney L, 'Discrimination in Online Ad Delivery' (28 January 2013) <https://arxiv.org/pdf/1301.6822.pdf> accessed 19 October 2017.

Takahashi A, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR* (1st edn, Intersentia, Antwerp 2002).

Taylor E, 'The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality' (January 2016) <https://www.cigionline.org/sites/default/files/gcig_no24_web_2.pdf> accessed 19 October 2017.

Taylor L, Floridi L, and van der Sloot B, 'Introduction: A New Perspective on Privacy' in Linnet Taylor, Luciano Floridi, and Bart van der Sloot (eds) *Group Privacy New Challenges of Data Technologies* (Springer Nature 2017).

Taylor M, 'The EU's human rights obligations in relation to its data protection laws with extraterritorial effect' (2015) International Data Privacy Law 5:4 246.

Taylor N, 'Policing, privacy and proportionality' (2003) European Human Rights Law Review 86.

Techopedia, 'What is a Virtual Internet Service Provider? <https://www.techopedia.com/definition/2540/virtual-internet-service-provider-visp> accessed 7 December 2015.

-- 'What is a Home Area a Network?' <https://www.techopedia.com/definition/26043/home-area-network-han> accessed 30 November 2015.

Tene O and Polonetsky J, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) Northwestern Journal of Technology and Intellectual Property 11:5 239.

The Conservative Party, 'A real vote-winner' <https://www.facebook.com/business/success/conservative-party> accessed 18 April 2018.

The Council of Bars and Law Societies of Europe, 'Comments on the Draft Framework Decision On the Retention of Data' (February 2005) <http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/lobbying_paper_data_1_1182260611.pdf> accessed 25 May 2017.

The Draft Data Retention and Acquisition Regulations 2018 SI 2018.

The Economist, 'Clever cities The multiplexed metropolis' *The Economist* (London, 5 September 2013) <https://www.economist.com/news/briefing/21585002-enthusiasts-think-data-services-can-change-cities-century-much-electricity?frsc=dg/a> accessed 2 September 2017.

The Guardian, 'New law would force Facebook and Google to give police access to encrypted messages' *The Guardian* (London, 14 July 2017) <https://www.theguardian.com/technology/2017/jul/14/new-law-would-force-facebook-and-google-to-give-police-access-to-encrypted-messages?CMP=share_btn_tw> accessed 12 April 2018.

Tijhaar R.F, 'Data retention and the right to privacy, happily ever after? What the European Court of Justice and European Court of Human Rights teach us' (May 2018) <http://arno.uvt.nl/show.cgi?fid=145932> accessed 10 October 2018.

Thomas C, 'Ethnicity and the Fairness of Jury Trialsin England and Wales 2006-2014' (2017) Criminal Law Review 11 860.

Thomas W, 'There is only one presumption of innocence' (2013) Neth J Leg Philos 42:3 193.

Timm, 'The government just admitted it will use smart home devices for spying' *The Guardian* (London, 9 February 2016) <https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government> accessed 8 December 2017.

Tompkins P and Lawley J, 'Context Matters' (5 April 2003) <http://www.cleanlanguage.co.uk/articles/articles/205/1/Context-Matters/Page1.html> accessed 3 April 2017.

Tor, ‘Tor on Android’ <https://www.torproject.org/docs/android.html.en> accessed 10 March 2018..

Trade and Industry Committee, *UK Online Reviewed: the First Annual Report of the E-Minister and E-Envoy Report* (HC 66 1999-2000.

Travis A, ‘Snooper's charter: GCHQ will be licensed 'to hack a major town' *The Guardian* (London, 21 June 2016) <https://www.theguardian.com/world/2016/jun/21/snoopers-charter-gchq-would-be-licensed-for-bulk-hacking> accessed 7 August 2017.

Tumay M, ‘The Concept Of ‘Necessary In A Democratic Society’ In Restricton Of Fundamental Rights A Reflection From European Convention On Human Rights’ (2011) Human Rights Review I:2.

Tunley M, Whittaker A, Gee J and Button M, *The Accredited Counter Fraud Specialist Handbook* (John Wiley & Sons 2014).

Turow J, Hennessy M and Draper N, ‘The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening them up to Exploitation’ (June 2015) <https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_2.pdf> accessed 4 October 2017

Tyner J.A, ‘Self and space, resistance and discipline: a Foucauldian reading of George Orwell's 1984’ (2004) Social & Cultural Geography 5:1 129.

Tzanou M, ‘Is Data Protection the Same as Privacy? An Analysis of Telecommunications’ Metadata Retention Measures’ (2013) Journal of Internet Law 17:3 20.

Uglow S, ‘The Human Rights Act 1998: Part 4: covert surveillance and the European Convention on Human Rights,’ [1999] Criminal Law Review 287.

United Nations General Assembly, ‘The promotion, protection and enjoyment of human rights on the Internet’ (27 June 2016) <https://www.article19.org/data/files/Internet_Statement_Adopted.pdf> accessed 25 April 2017.

Uteck A, “Ubiquitous Computing and Spatial Privacy” in Ian Kerr *et. al.*, eds., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford: Oxford University Press, 2009).

Vainio N and Miettinen S, ‘Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States’ (2015) International Journal of Law and Information Technology 23:3 290.

van der Hilst R, ‘Human Rights Risks of Selected Detection Technologies Sample Uses by Governments of Selected Detection Technologies’ (2009) <http://www.detecter.bham.ac.uk/D17.1HumanRightsDetectionTechnologies.doc> accessed 26 April 2017,

-- 'Characteristics and uses of selected detection technologies, including their potential human rights' (30 November 2011) <http://www.detecter.bham.ac.uk/pdfs/17_3_tracking_technologies.doc> accessed 13 April 2017.

-- 'Ranking, in terms of their human rights risks, the detection technologies and uses surveyed in WP09' (2011) <http://www.detecter.bham.ac.uk/pdfs/17_4_human_rights_ranking_of_technologies.doc> accessed 12 May 2017.

van der Leun J.P and van der Woude M.A.H, 'Ethnic profiling in the Netherlands? A reflection on expanding preventive powers, ethnic profiling and a changing social and political context' (2011) Policing and Society 21:4 444

van der Schyff G, 'Interpreting the protection guaranteed by two-stage rights in the European Convention on Human Rights: The case for wide interpretation' in Eva Breams and Janneke Gerards (eds) *Shaping Rights in the ECHR: The Role of the European Court of Human Rights in Determining the Scope of Human Rights* (Cambridge University Press 2013).

van der Sloot B, 'Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?' (2014) JIPITEC 230.

-- 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) International Data Privacy Law 4:4 307.

-- 'Privacy as human flourishing Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?' (2014) Journal of Intellectual Property, Information Technology and E-Commerce Law 230.

-- 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"' (2015) Utrecht Journal of International and European Law 31:80 25.

-- 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move* (Springer 2016).

-- 'Decisional privacy 2.0: the procedural requirements implicit in Article 8 ECHR and its potential impact on profiling' (2017) International Data Privacy Law 0:0 1.

-- '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 Linnet Taylor, Luciano Floridi, and Bart van der Sloot (eds) *Group Privacy New Challenges of Data Technologies* (Springer Nature 2017).

van der Sloot B, Broeders D and Schrijvers E, *Exploring the Boundaries of Big Data* (Amsterdam University Press, Amsterdam 2016).

van Dijk A.A, 'Retributivist Arguments against Presuming Innocence' (2013) Neth J Leg Philos 42:3 249.

van Gulijk C *et al*, 'SURVEILLE Paper Assessing Surveillance in the Context of Preventing a Terrorist Act' (29 May 2017) <https://www.justsecurity.org/wp-content/uploads/2014/10/SURVEILLE-Paper-on-a-Terrorism-Prevention.pdf> accessed 14 June 2017.

van Rijsbergen K, 'The effectiveness of a homemade IMSI catcher build with YateBTS and a BladeRF' (2015) <http://www.delaat.net/rp/2015-2016/p86/report.pdf> accessed 10 October 2017.

van Zyl Smit J, 'The New Purposive Interpretation of Statutes: HRA Section 3 after Ghaidan v Godin-Mendoza' (2007) MLR 70:2 294.

Vedaschi A and Lubello V, 'Data Retention and its Implications for the Fundamental Right to Privacy' (2015) Tilburg Law Review 20 14, 16.

Vick D, 'Interdisciplinarity and the Discipline of Law' (2004) 31 JL & Soc 163,

Vilasau M, 'Directive 2006/24 / EC on data retention of electronic communications traffic: safety vs. privacy' (2006) IDP. Journal of Internet Law and Policy 0:3.

Villegas M.O, 'Introduction to next-generation firewalls in the enterprise' *TechTarget* (February 2015) <http://searchsecurity.techtarget.com/feature/Introduction-to-next-generation-firewalls-in-the-enterprise> accessed 6 December 2017.

Vincent J, 'The UK Now Wields Unprecedented Surveillance Powers – Here's what it means' *The Verge* (Manhattan, New York City, 29 November 2016) <https://www.theverge.com/2016/11/23/13718768/uk-surveillance-laws-explained-investigatory-powers-bill> accessed 8 January 2018.

Vincents O.B, 'Interception of internet communications and the right to privacy: an evaluation of some provisions of the Regulation of Investigatory Powers Act against the jurisprudence of the European Court of Human Rights' (2007) E.H.R.L.R. 6 637.

Vorratsspeicherung, 'Study finds telecommunications data retention ineffective' (27 Jan 2011) <http://www.vorratsdatenspeicherung.de/content/view/426/79/lang,en/> accessed 29 July 2017.

-- 'Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics' (19 February 2011) <http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf> accessed 29 July 2017.

Walker C and Akdeniz Y, 'Anti-Terrorism Laws and Data Retention: War is over?' (2003) Northern Ireland Legal Quarterly 54:2 159.

Walsh C, 'Psychedelics and Cognitive Liberty: reimagining drug policy through the prism of human rights' (2016) International Journal of Drug Policy 29: 80.

Wachter S, 'Privacy: Primus Inter Pares Privacy as a precondition for self-development, personal fulfilment and the free enjoyment of fundamental human rights' (2017) Oxford Internet Institute < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903514 > accessed 1 December 2017.

Watson C and Ingram B, 'The Twitter Joke Judgment: The Law with Unintended Consequences?' (17 August 2012) <http://www.scl.org/site.aspx?i=ed27370> accessed 1 December 2017.

Weber L and Bowling B, *Stop and Search: Police Power in Global Context* (Routledge 2012).

Whatsapp, 'How do I use Group Chat?' <https://www.whatsapp.com/faq/en/iphone/23782517> accessed 10 May 2017.

White M, 'The new Opinion on Data Retention: Does it protect the right to privacy?' (27 July 2016) < http://eulawanalysis.blogspot.co.uk/2016/07/the-new-opinion-on-data-retention-does.html> accessed 1 November 2016.

-- 'When can EU citizens be expelled from the UK after Brexit? The Human Rights Dimension' (4 October 2016) <https://eulawanalysis.blogspot.co.uk/2016/10/when-can-eu-citizens-be-expelled-from.html> accessed 14 May 2017.

-- 'Protection by Judicial Oversight, or an Oversight in Protection?' (2017) Journal of Information Rights, Policy and Practice 2:1 1.

-- 'The Privacy International case in the IPT: respecting the right to privacy?' (14 September 2017) <https://eulawanalysis.blogspot.co.uk/2017/09/the-privacy-international-case-in-ipt.html> accessed 3 January 2018.

-- 'Data Retention is still here to stay, for now…' (5 February 2018) <https://eulawanalysis.blogspot.co.uk/2018/02/data-retention-is-still-here-to-stay.html> accessed 1 June 2018.

-- 'Guest post: Data Retention: I can't believe it's not lawful, can you? A response to Anthony Speaight QC' (2 March 2018) <https://paulbernal.wordpress.com/2018/03/02/guest-post-data-retention-i-cant-believe-its-not-lawful-can-you-a-response-to-anthony-speaight-qc/> accessed 9 April 2018.

-- 'Proposed police super-database breaks the law and has no legal basis – but the Home Office doesn't care' (9 October 2018) <https://theconversation.com/proposed-police-super-database-breaks-the-law-and-has-no-legal-basis-but-the-home-office-doesnt-care-104527> accessed 11 October 2018.

Wildhaber L, 'Dialogue Between Judges' (2006) <http://www.echr.coe.int/Documents/Dialogue_2006_ENG.pdf> accessed 4 October 2017.

Wilding R, ''Virtual' intimacies? Families communicating across transnational contexts' (2006) Global Networks 6:2 125.

Williams A.L and Merten M.J, 'iFamily: Internet and Social Media Technology in the Family Context' (2011) Family & Consumer Sciences Research Journal 40:2 150

Williams C, 'BT and Phorm: how an online privacy scandal unfolded' *The Telegraph* (London, 8 April 2011) <http://www.telegraph.co.uk/technology/news/8438461/BT-and-Phorm-how-an-online-privacy-scandal-unfolded.html> accessed 17 April 2017.

Williams R and Johnson P, 'Circuits of Surveillance' (2004) Surveillance & Society 2:1 1.

Wisman T, 'Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things' (2013) EJLT 4:2 <http://ejlt.org/article/view/192/379> accessed 2 May 2017.

-- 'Privacy: Alive and Kicking' (2015) European Data Protection Law Review 1:1 80.

Wilson D, 'I exposed corruption at War Child. Here's why whistleblowers need anonymity' *The Guardian* (London, 10 April 2017) <https://www.theguardian.com/voluntary-sector-network/2017/apr/10/whistleblower-war-child-need-anonymity-corruption> accessed 5 May 2017.

Wood D.M and Webster C.W.R, 'Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain's Bad Example' (2009) Journal of Contemporary European Research 5:2 259.

Wood D, Apthorpe N and Feamster N, 'Cleartext Data Transmissions in Consumer IoT Medical Devices' (2017) IoT S&P'17 7.

Woods L, 'Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)' (21 December 2016) <https://eulawanalysis.blogspot.co.uk/2016/12/data-retention-and-national-law-ecj.html> accessed 21 June 2017.

World Heritage Convention, 'From the Great Saltworks of Salins-les-Bains to the Royal Saltworks of Arc-et-Senans, the Production of Open-pan Salt' <http://whc.unesco.org/en/list/203> accessed 21 November 2017.

Wortmann F, and Flüchter K, 'Internet of Things - Technology and Value Added' (2015) Business & Information Systems Engineering 57:3 221.

Written evidence from Dr Julian Huppert, University of Cambridge (IPB0027).

Written evidence: IT-Political Association of Denmark (IPB20).

Written evidence submitted by Andrews & Arnold Ltd (IPB0011).

Written evidence submitted by Big Brother Watch (IPB0048).

Written evidence submitted by BT (IPB0061).

Written evidence submitted by Exa Networks Limited (IPB0026).

Written evidence submitted by Gareth Llewellyn on behalf of Brass Horn Communications (IPB0019).

Written evidence submitted by Graham Smith (IPB0025.

Written evidence submitted by GreenNet (IPB0063).

Written evidence submitted by IT-Political Association of Denmark (IPB0051).

Written evidence submitted by Open Rights Group (IPB0034).

Written evidence submitted by the Electronic Frontier Foundation (IPB0017).

Written evidence submitted by The Institute for Human Rights and Business (IHRB) (IPB0035).

Written evidence submitted by the Institute for Human Rights and Business written evidence (IPB0094).

Written evidence submitted by Tim Panton (IPB0016).

York J, 'The harms of surveillance to privacy, expression and association' (2014) <https://giswatch.org/en/communications-surveillance/harms-surveillance-privacy-expression-and-association> accessed 12 May 2017.

Yourow H.C, *The Margin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence* (1st edn, Martinus Nijhoff Publishers, 1996).

Zeit Online, 'Tell-all telephone' <http://www.zeit.de/datenschutz/malte-spitz-data-retention> accessed 13 April 2017.

Ziemele I, 'Conclusions' in Iulia Motoc and Ineta Ziemele (eds) *The Impact of the ECHR on Democratic Change in Central and Eastern Europe* (Cambridge University Press 2016).

Zittrain J, 'Facebook Could Decide an Election Without Anyone Ever Finding Out' *The New Republic* (New York City, 2 June 2014) <https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering> accessed 25 November 2017.

Zöller V, 'Liberty Dies by Inches: German Counter-Terrorism Measures and Human Rights' (2004) German Law Journal 5:5 469.

Zuboff S, *In the age of the smart machine: the future of work and power* (New York: Basic Books 1988).

-- 'Big Other: Surveillance capitalism and the prospects of an information civilization' (2015) Journal of Information Technology 30:1 75.

-- ‘The Secrets of Surveillance Capitalism’ (5 March 2016) <http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html> accessed 22 February 2017.

Table of Cases

Beghal v DPP [2015] UKSC 49.

Belgian Linguistic Case (No.2) App nos. 1474/62, 1677/62, 1691/62, 1769/63, 1994/63, 2126/64 (ECHR, 23 July 1968).

Bernh Larsen Holding AS and Others v. Norway App no. 24117/08 (ECHR, 14 March 2013)

Big Brother Watch v UK App nos. 58170/13, 62322/14 and 24960/15 (ECHR, 13 September 2018).

Biržietis v Lithuania App no. 49304/09 (ECHR, 14 June 2016).

Botta v Italy App no. 21439/93 (ECHR, 24 February 1998.

Brennan v UK App no. 39846/98 (ECHR, 16 October 2001).

Breyer v Germany App no. 50001/12 Communicated on 21 March 2016.

Bulgaria Constitutional Court, Decision no. 8/2014, 12 March 2015.

Buscarini and Others v San Marino App no. 24645/94 (ECHR, 18 February 1999).

BVerfG, judgment of the First Senate of 02 March 2010 - 1 BvR 256/08 - Rn. (1-345).

Campanelli v Italy App no. 25358/12 (ECHR, 24 January 2017).

Campbell and Cosans v the United Kingdom App no 3578/05 (ECHR, 25 February 1982).

Carpenter v. United States, No. 16-402, 585 U.S. ____ (2018).

Carson and Others v UK App no. 42184/05 (ECHR, 16 March 2010).

Case C-155/79 *AM & S Europe Limited v Commission of the European Communities Legal privilege* [1982] ECR I-01575.

Case-162/97 *Nilsson & Ors (Agriculture)* [1998] ECR I-7477.

Case-308/97 *Manfredi (Agriculture)* [1998] ECR I-7685.

Case C‑275/06 *Promusicae v Telefónica de España SAU* [2007] ECR I-00271, Opinion of Kokott.

Case C-127/08, *Metock v Minister of Justice, Equality and Law Reform* [2008] ECR I-06241.

Case C-301/06 *Ireland v Parliament and Council* [2009] ECR I-00593.

Case C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063.

Case C-131/12, *Google Spain SL v Agencia Española de Protección de Datos, González* [2014] E.C.R. 317.

Case C‑362/14 *Schrems* [2015] ECR-I 650.

Case C‑698/15 Order of the President of the Court (Expedited procedure), 1 February 2016.

Case C‑582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECR I-779.

Case C-73/16 *Puškár* [2017] ECR I-253, Opinion of Advocate General Kokott.

Case C-207/16 *Ministerio Fiscal* [2018] ECR-I 300, Opinion of Saugmandsgaard Øe.

Case C-207/16 *Ministerio Fiscal*.

Case C-623/17 *Ministerio Fiscal*.

Case- T-102/96 *Gencor Ltd v Commissio* [1999] ECR II-0753.

Catt and T, R (on the applications of) v Commissioner of Police of the Metropolis [2015] UKSC 9.

Centrum För Rättvisa v Sweden App no. (ECHR, 19 June 2018).

C.G. and others v Bulgaria App no. 1365/07 (ECHR, 24 April 2008).

CG v Facebook Ireland Ltd & McCloskey [2016] NICA 54.

Chambers v Director of Public Prosecutions [2012] EWHC 2157 (Admin).

Chassagnou v France App nos. 25088/94, 28331/95 and 28443/95 (ECHR, 29 April 1999).

Clift v UK App no. 7205/07 (ECHR, 13 July 2010).

Colon v Netherlands App no 49458/06 (ECHR, 15 May 2012).

Commonwealth v. Thorpe, 424 N.E.2d 250 (1981).

Communist Party of Russia and Others v Russia App no. 29400/05 (ECHR, 19 June 2012).

Copland v UK App no. 62617/00 (ECHR, 3 April 2007).

Costel Popa v Romania App no. 47558/10 (ECHR, 26 April 2016).

Countryside Alliance v and others, R (on the application of) v Attorney General & Anor [2007] UKHL 52.

Cyprus v Turkey App no. 25781/94 (ECHR, 10 May 2001).

Davis & Ors, R (on the application of) v Secretary of State for the Home Department & Ors [2015] EWHC 2092.

Davis & Ors, R (on the application of) v Secretary of State for the Home Department & Ors [2015] EWCA Civ 1185.

Decision G 47/2012-49, G 59/2012-38, G 62/2012-46, G 70/2012-40, G 71/2012-36 27 June 2014.

Decision of the District Court of The Hague, Case Number C/09/480009 KG ZA 14/1575, 11 March 2015.

Delfi AS v Estonia App no. 64569/09 (ECHR, 16 June 2015).

Demades v Turkey App no. 16219/90 (ECHR, 31 July 2003).

Demir and Baykara v Turkey App no. 34503/97 (ECHR, 12 November 2008).

De Tommaso v Italy App no. 43395/09 (ECHR, 23 February 2017).

Deweer v Belgium App no. 6903/75 (ECHR, 27 February 1980).

D.H. and Others v the Czech Republic App no. 57325/00 (ECHR, 13 November 2007).

Djavit v Turkey App no. 20652/92 (ECHR, 20 February 2003).

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

Doerga v Netherlands App no. 50210/99 (ECHR, 27 April 2004).

Dragojević v Croatia App no. 68955/11 (ECHR, 15 January 2015).

Draksas v Lithuania App no. 36662/04 (ECHR, 31 July 2002).

Eckle v Germany App no. 8130/78 (ECHR, 15 July 1982).

Ekin Associations v France App no. 39288/98 (ECHR, 17 July 2001).

El-Masri v The Former Yugoslav Republic of Macedonia App no. 39630/09 (ECHR, 13 December 2012).

Engel and Others v UK App nos. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72 (ECHR, 8 June 1976).

Erményi v Hungary App no. 22254/14 (ECHR, 22 November 2016).

Ernst and Others v Belgium App no. 33400/96 (ECHR, 15 July 2003).

Faber v Hungary App no. 40721/08 (ECHR, 24 July 2012).

Fernández Martínez v Spain App no. 56030/07 (ECHR, 12 June 2014).

Folgerø and Others v Norway App no. 15472/02 (ECHR, 29 June 2007).

Folberø and Others v Norway App no. 15472/02 (ECHR, 29 June 2007).

Geotech Kancev GMBH v Germany App no. 23646/09 (ECHR, 2 June 2016).

Ghaidan v Godin-Mendoza [2004] UKHL 30.

Gillan and Quinton v UK App no. 4158/05 (ECHR, 12 January 2010).

Glas Nadezhda Eood and Anatoliy Elenkov v Bulgaria App no. 14134/02 (ECHR, 11 October 2007).

Glor v Switzerland App no. 13444/04 (ECHR, 30 April 2009).

Gorzelik and Others v Poland App no. 44158/98 (ECHR, 17 February 2004).

Gough v UK App no. 49327/11 (ECHR, 28 October 2014).

Greuter v the Netherlands App no. 40045/98 (ECHR, 19 March 2002).

Groppera Radio AG and others v Switzerland App no. 10890/84 (ECHR, 28 March 1990).

Guja v Moldova App no. 14277/04 (ECHR, 12 February 2008).

Güneri and Others v Turkey App no. 42853/98 (ECHR, 12 July 2005).

Halford v UK App no. 20605/92 (ECHR, 25 June 1997).

Handyside v United Kingdom App no. 5493/72 (ECHR, 7 December 1976).

Hasan and Chaush v Bulgaria App no. 30985/96 (ECHR, 26 October 2000).

Hatton v UK App no. 36022/97 (ECHR, 8 July 2003).

Hirst v UK App no. 74025/01 (ECHR, 6 October 2005).

Human Rights Watch & Others v The Secretary of State for the Foreign & Commonwealth Office & Others [2016] IPT/15/165/CH, IPT/15/166 CH, IPT/15/167/CH, IPT/15/168/CH, IPT/15/169/CH, IPT/15/172/CH, IPT/15/173/CH, IPT/15/174/CH, IPT/15/175/CH, IPT/15/176/CH.

Huvig v France App no. 11105/84 (ECHR, 24 April 1990).

Ibrahimov and Others v Azerbaijan App nos. 69234/11 69252/11 69335/11 (ECHR, 11 February 2016).

Ilgar Mammadov v Azerbaijan App no. (ECHR, 22 May 2014).

Iordachi v Moldova App no. 25198/02 (ECHR, 10 February 2009).

Ismail DUYGULU v Turkey App no. 4667/03 (ECHR, 20 November 2007).

Ivanova v Bulgaria App no. 52435/99 (ECHR, 12 April 2007).

Janowiec and Others v Russia App nos. 55508/07 and 29520/09 (ECHR, 21 October 2013).

Jehova's witnesses of Moscow v Russia App no. 302/02 (ECHR, 10 June 2010).

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] ECR I-845, Opinion of Cruz Villalón.

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECR I-238.

Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-572, Opinion of Saugmandsgaard Øe.

Joined Cases C‑203/15 and C‑698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-970.

Kafkaris v Cyrprus App no. 21906/04 (ECHR, 12 February 2008).

Kennedy v UK App no. 26839/05 (ECHR, 18 May 2010).

Khlyustov v Russia App no. 28975/05 (ECHR, 11 July 2013).

Khodorkkovsky and Lebedev v Russia App nos. 11082/06 and 13772/05 (ECHR, 25 July 2013).

Khuzhin and Others v Russia App no. 13470/02 (ECHR, 23 October 2008).

Klass v Germany App no. 5029/71 (ECHR, 6 September 1978).

Klayman v Obama, 2013 WL 6571596 (D.D.C. Dec. 16, 2013).

Kopp v Switzerland App no. 23224/94 (ECHR, 25 March 1998).

KU v Finland App no. 2872/02 (ECHR, 2 December 2008).

Kruslin v France App no. 11801/85 (ECHR, 24 April 1990).

Kudrevićius and Others v Lithuania App no. 37553/05 (ECHR, 15 October 2015).

Kurić and others v Slovenia App no. 26828/06 (ECHR, 12 March 2013).

Laskey, Jaggard and Brown v UK App nos. 21627/93 21826/93 21974/93 (ECHR, 19 February 1997).

L.C.B. v UK App no. 23413/94 (ECHR, 9 June 1998).

Leander v Sweden App no. 9248/81 (ECHR, 26 March 1987).

Liberty and Others v Government Communication Head Quarters and Others [2014] UKIPTrib 13_77-H, 5 December 2014.

Liberty and Others v UK App no. 58243/00 (ECHR, 1 July 2008).

Liberty v Secretary of State for the Home Department and Others [2018] EWHC 975.

Lingens v Austria App no. 9815/82 (ECHR, 8 July 1986).

Loizidou v Turkey App no. 15318/89 (ECHR, 23 March 1995).

LS, R (on application of) v South Yorkshire Police (Consolidated Appeals) [2004] UKHL 39.

Magyar Helsinki Bizottsag v Hungary App no. 18030/11 (ECHR, 8 November 2016).

Malone v UK App no. 8691/79 (ECHR, 2 August 1984).

Marcel and Others v Commissioner of Police of the Metropolis and Others [1991] 2 W.L.R. 1118, [1130].

Marper & Anor, R (on the application of) v Chief Constable of South Yorkshire & Anor [2002] EWCA Civ 1275.

Mathieu-Mohin and Clerfayt v Belgium App no. 9267/81 (ECHR, 2 March 1987).

McCann and Others v UK App no. 18984/91 (ECHR, 27 September 1995).

McE, Re (Northern Ireland) [2009] UKHL 15.

McFarlane v Ireland App no. 31333/06 (ECHR, 10 September 2010).

McFeeley v UK App no. 8317/78 (ECHR, 15 May 1980).

McKay v the United Kingdom App no. 543/03 (ECHR, 3 October 2006).

Michaud v France App no. 12323/11 (ECHR, 6 December 2012.

Mills & Anor, R (on the application of) v Sussex Police & Anor [2014] EWHC 2523.

M.K. v France App no. 19522/09 (ECHR, 18 April 2013).

M.L. v Germany and W.W. v Germany App nos. 60798/10 and 65599/10, communicated to the respondent Government under Article 8 of the Convention on 29 November 2012.

MM v UK App no. 24029/07 (ECHR, 13 November 2012).

Moohan and Gillon v UK App nos. 22962/15 23345/15 (ECHR, 13 June 2017).

Mosely v UK App no. 48009/08 (ECHR, 10 May 2011).

Mouvement raëlien Suisse v Switzerland App no. 16354/06 (ECHR, 13 July 2012).

Murphy v Ireland App no. 44179/98 (ECHR, 10 July 2003).

Mustafa Sezgin Tanrikulu v Turkey App no. 27473/06 (ECHR, 18 July 2017).

Nachova and Others v Bulgaria App nos. 43577/98 and 43579/98 (ECHR, 6 July 2005).

Nada v Switzerland App no. 10593/08 (ECHR, 12 September 2012).

Niemetz v Germany App no. 13710/88 (ECHR, 16 December 1992).

Niyazov v Russia App no. 27843/11 (ECHR, 16 October 2012).

Nolan and K v Russia App no. 2512/04 (ECHR, 12 February 2009).

Norman Baker v the Information Commissioner and the Cabinet Office [2006] EA/2006/0045.

N v UK App no. 26565/05 (ECHR, 27 May 2008).

Oršuš and Others v Croatia App no. 15766/03 (ECHR, 16 March 2010).

Osman v UK App no. 23452/94 (ECHR, 28 October 1998).

Pantea v Romania App no. 33343/96 (ECHR, 3 June 2003).

Petrov v Bulgaria App no. 15197/02 (ECHR, 22 May 2008).

'Population Census Decision', Judgment of 15 December 1983, 1 BvR 209/83, BVerfGE 65.

Pretty v UK App no. 2346/02 (ECHR, 29 April 2002).

Privacy International v the Secretary of State for Foreign and Commonwealth Affairs and Others [2017] IPT/15/110/CH.

Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others [2016] UKIPTrib 15_110-CH.

Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others [2018] UKIPTrib IPT_15_110_CH.

Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others [2018] IPT/15/110/CH.

Pullen & Ors -v- Dublin City Council [2008] IEHC 379.

Refah Partisi (The Welfare Party) and Others v Turkey App nos. 41340/98, 41342/98, 41343/98 and 41344/98 (ECHR, 13 February 2003).
R. v. Orlandis-Habsburgo, 2017 ONCA 64.

R v Spencer [2014] 2 SCR 212.

Re: a complaint of surveillance [2013] IPT/A1/2013.

Rekvényi v Hungary App no. 25390/94 (ECHR, 20 May 1999).

Reiner v Bulgaria App no. 46343/99 (ECHR, 23 May 2006).

Request for a preliminary ruling from the Audiencia provincial de Tarragona, Sección cuarta (Spain) lodged on 14 April 2016 — *Ministerio Fiscal* (Case C-207/16).

Request for a preliminary ruling from the Kammarrätten i Stockholm (Sweden) lodged on 4 May 2015 — *Tele2 Sverige AB v Post- och telestyrelsen* (Case C-203/15).

Reference for a preliminary ruling from the Investigatory Powers Tribunal — London (United Kingdom) made on 31 October 2017 — *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*.

R.E. v United Kingdom App no. 62498/11 (ECHR, 27 October 2015).

RJM, R (On The Application of) v Secretary of State For Work and Pensions [2008] UKHL 63.

Romania Constitutional Court DECISION no.12581 from 8 October 2009.

Romania Constitutional Court, Decision no. 653, 8 July 2014.

Romanava v Russia App no. 23215/02 (ECHR, 11 October 2011).

Roman Zakharov v Russia App no. 47143/06 (ECHR, 4 December 2015).

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

S & Anor, R v [2008] EWCA Crim 2177.

Sahin v Germany App no. 30943/96 (ECHR, 8 July 2003).

S.A.S v France App no. 43835/11 (ECHR, 1 July 2014).

Sakhnovskiy v Russia App no. 21272/03 (ECHR, 2 November 2010).

S and Marper v UK App nos. 30562/04 and 30566/04 (ECHR, 4 December 2008).

Sanoma Uitgevers B.V. v the Netherlands App no. 38224/03 (ECHR, 14 September 2010).

Saunders v UK App no. (ECHR, 17 December 1996).

Satakunnan Markkinapörssi Oy and Satamedia Oy v v Finland App no. 931/13 (ECHR, 27 June 2017).

Schweizerische Radio- und Fernsehgesellschaft SRG v Switzerland App no. 34124/06 (ECHR, 21 June 2012).

Secretary of State for the Home Department v Davis MP & Ors [2015] EWCA Civ 1185.

Secretary of State for the Home Department v Rehman [2001] UKHL 47.

Sefilyan v Armenia App no. 22491/08 (ECHR, 2 October 2012).

Segerstedt-Wiberg and Others v Sweden App no. 62332/00 (ECHR, 6 June 2006).

Shimovolos v Russia App no. 30194/09 (ECHR, 21 June 2011).

Silver and Others v UK App nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 and 7136/75 (ECHR, 25 March 1983).

Sinan Isik v Turkey App no. 21924/05 (ECHR, 2 February 2010).

Singh, R (on the application of) v Chief Constable of West Midlands Police [2006] EWCA Civ 1118.

Smith and Grady v United Kingdom App nos. 33985/96; 33986/96 (ECHR, 27 September 1999).

Smyth, Re Judicial Review [2017] NIQB 55.

Société Colas Est and others v France App no. 37971/97 (ECHR, 16 April 2002).

Soering v UK App no. 14038/88 (ECHR, 7 July 1989).

Soltysyak v Russia App no. 4663/05 (ECHR, 10 February 2011).

Sommerfield v Germany App no. 31871/96 (ECHR, 8 July 2003).

Sørensen and Rasmussen v Denmark App nos. 52562/99 and 52620/99 (ECHR, 11 January 2006).

Stafford v United Kingdom App no. 46295/99 (ECHR, 28 May 2002).

Sunday Times v United Kingdom App no. 6538/74 (ECHR, 26 April 1979).

Sunday Times v UK (No.2) App no. 13166/87 (ECHR, 26 November 1991).

Surikov v Ukraine App no. 42788/06 (ECHR, 26 January 2017).

S. v Switzerland App nos. 12629/87 13965/88 (ECHR, 28 November 1981).

Szabó and Vissy v Hungary App no. 37138/14 (ECHR, 12 January 2016).

Szuluk v UK App no. 36936/05 (ECHR, 2 June 2009).

Telegraaf and Others v the Netherlands App no. 39315/06 (ECHR, 22 November 2012).

Tillack v Belgium App no. 20477/05 (ECHR, 27 November 2007).

The Constitutional Court of the Republic of Slovenia, U-I-65/13-19 of 3 July 2014.

The Czech Republic Constitutional Court 2011/03/22 - Pl. ÚS 24/10.

The Law Society, Hine Solicitors and Kevin McGrath v Rick Kordowski [2011] EWHC 3185 (QB).

Thlimmenos v Greece App no. 34369/97 (ECHR, 6 April 2000).

Tom Watson and Others v Secretary of State for the Home Department [2018] EWCA Civ 70.

.

Tryer v United Kingdom App no. 5856/72 (ECHR, 25 April 1978).

Tillack v Belgium App no. 20477/05 (ECHR, 27 November 2007).

United Communist Part of Turkey and Others v Turkey App no. 19392/92 (ECHR, 30 January 1998).

Uzun v Germany App no. 35623/05 (ECHR, 2 September 2010).

Valenzuela Contreras v Spain App no. 27671/95 (ECHR, 30 July 1998).

Vaughan v South Oxfordshire District Council [2012] IPT/12/28/C.

Vilvarajah and Others v UK - App nos. 13163/87; 13164/87; 13165/87; 13447/87; 13448/87), 30/10/1991, (ECHR, 30 October 1991).

Weber and Saravia v Germany App no. 54934/00 (ECHR, 29 June 2006).

X v Iceland App no. 6825/74 (ECHR, 18 May 1976).

X, Y and Z v UK App no. 21830/93 (ECHR, 22 April 1997).

Young, James and Webster v UK App nos. 7601/76 and 7896/77 (ECHR, 14 December 1979).

Youth Initiative for Human Rights v Serbia App no. (ECHR, 25 June 2013).

Z v Finland App no. 22009/93 (ECHR, 25 February 1997).

Zdanoka v Latvia App no. 58278/00 (ECHR, 16 March 2006).

Table of Statutes

Charter of Fundamental Rights of the European Union.

Council of Europe's Convention on Cybercrime ETS No. 185, 23.XI.2001.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series no. 108, Strasbourg, 1981.

Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 4.XI.1950.

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

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

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.

European German Basic Law.

Federal Law No. 374.

Federal Law No. 375-FZ.

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

The Telecommunications Act 1984.

The Interception of Communications Act 1985.

The Regulation of Investigatory Powers Act 2000.

The Anti-Terrorism, Crime and Security Act 2001.

The Anti-social Behaviour Act 2003.

The Communications Act 2003.

The Data Retention and Investigatory Powers Act 2014.

The Counter-Terrorism and Security Act 2015.

The Investigatory Powers Act 2016.

The EU (Withdrawal) Act 2018.

The Data Retention (EC Directive) Regulations 2007 SI 2007 No. 2199.

The Data Retention (EC Directive) Regulations 2009 SI 2009 No. 859.