NOTE

DIGITAL RIGHTS IRELAND DÈJA VU?: WHY THE BULK ACQUISITION WARRANT PROVISIONS OF THE INVESTIGATORY POWERS ACT 2016 ARE INCOMPATIBLE WITH THE CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

RUBIN S. WARANCH*

> Awareness that the Government may be watching chills associational and expressive freedoms . . . . I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.[1]

INTRODUCTION

Think of every website you have visited in the last week, or month, or year. Think about the countless emails and text messages you have sent and the number of phone calls you have made. Now imagine that the government has access to the metadata of all of these communications—all the information except the actual content.[2] If this does not frighten you, consider the statement of the former U.S. National Security Agency (NSA) Director, Michael Hayden: "We kill people based on metadata."[3]

Hayden made this statement approximately one year after Edward Snowden's early revelations about the intelligence policies

* J.D. expected 2018, The George Washington University Law School; B.A. 2015, The University of Maryland, Baltimore County (UMBC).

1. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

2. *See* 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 United States*, 28 HARV. HUM. RTS. J. 65, 74 (2015). Metadata is defined as "data related to the source, addressee, date, time, length, and type of communication." *Id.*

3. David Cole, *'We Kill People Based on Metadata'*, NYR DAILY (Mar. 10, 2014), http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/ [https://perma.cc/Q58F-7D77].

of both the United States and the United Kingdom.[4] Snowden described the U.K.'s system as even "more intrusive to people's privacy than has been seen in the US."[5] One of his numerous leaks revealed that the U.K.'s Government Communications Headquarters (GCHQ) not only secretly collected and stored emails, Facebook posts, Internet records, and call histories of individuals—irrespective of whether they had ties to crime or terrorism—but that GCHQ also shared such information with the NSA.[6]

Shortly after Snowden's revelations, both the United States and United Kingdom justified their respective surveillance policies on public safety grounds.[7] However, while the United States backtracked on this stance in 2015 when President Barack Obama signed the Freedom Act into law,[8] the United Kingdom continued

---

4. *See generally* Paul Szoldra, *This is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks*, Bus. Insider (Sept. 16, 2016), http://www.businessinsider.com/snowden-leaks-timeline-2016-9 (providing a timeline of Snowden's revelations) [https://perma.cc/QHX9-25WQ]. In 2013, Edward Snowden leaked documents to the Guardian and the Washington Post regarding the U.S. National Security Agency's (NSA) PRISM program. *See* Gianluca Mezzofiore, *NSA Whistleblower Edward Snowden: Washington Snoopers are Criminals*, IB Times (June 17, 2013), http://www.ibtimes.co.uk/nsa-whistleblower-edward-snowden-479709 [https://perma.cc/9KRE-9DTK]. These insider documents revealed that PRISM permitted the NSA and Federal Bureau of Investigation to tap into major Internet providers' servers to extract private citizens' "audio and video chats, photographs, e-mails, documents, and connection logs." Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, Wash. Post (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.f7d382564b3f [https://perma.cc/F5LA-3YMK].

5. Carole Cadwalladr, *Edward Snowden: State Surveillance in Britain Has No Limits*, Guardian (Oct. 12, 2014), https://www.theguardian.com/world/2014/oct/12/snowden-state-surveillance-britain-no-limits [https://perma.cc/JD5U-GNWV].

6. *See* Ewen MacAskill et al., *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications*, Guardian (June 21, 2013), https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [https://perma.cc/XYG7-WRBN].

7. *See* Alan Travis, *Theresa May Defends Culture of Secrecy Over Mass Snooping*, Guardian (Oct. 16, 2014), https://www.theguardian.com/politics/2014/oct/16/theresa-may-secrecy-intelligence-services-spies (noting that Theresa May defended the U.K.'s surveillance policies) [https://perma.cc/TYJ9-GG5D]. U.S. officials, including former President Barack Obama, justified the program as a measure to prevent terrorist attacks. *See* Christopher York, *Barack Obama Justifies Prism NSA Surveillance Programme, Saying it Has Saved Lives*, Huffington Post U.K. (June 19, 2013), http://www.huffingtonpost.co.uk/2013/06/19/prism-obama-germany-merkel_n_3464613.html [https://perma.cc/NR2Q-JY6N].

8. Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (FREEDOM) Act of 2015, 50 U.S.C. § 1861 (2015) [hereinafter Freedom Act]. While this Note focuses on U.K. surveillance policies, the Freedom Act is a useful comparator that demonstrates how the United States limited the scope of when telecommunications providers would be forced to provide citizens' private data to intelligence agencies. *See* Nicole B. Cásarez, *The Synergy of Privacy and Speech*, 18 U. Pa. J. Const. L. 813, 815 (2016).

to defend its surveillance practices and marched towards a new expansive surveillance law—the Investigatory Powers Act 2016 (IP Act).[9] Prime Minister Theresa May provided a simple justification for the IP Act. She stated, "[i]f you are searching for the needle in the haystack, you have to have a haystack in the first place."[10]

The IP Act became official law after it received the Queen's royal assent[11] on November 29, 2016.[12] Since then, critics and supporters of the IP Act have articulated viewpoints that are in diametric opposition to one another.[13] Dr. Julian Huppert, a former Member of Parliament (MP), remarked that the IP Act is intrusive and impairs privacy rights.[14] Meanwhile, proponents of the IP Act applauded it as a transparent legal framework that permits intelligence agencies to combat terrorist and criminal activity.[15] This divide stems partially from the Court of Justice of the European Union's (CJEU) judgment in *Digital Rights Ireland v. Minister for Communications*.[16]

---

9. *See* Alan Travis, *Investigatory Powers Bill: Snooper's Charter to Remain Firmly in Place*, GUARDIAN (Nov. 2, 2015), https://www.theguardian.com/world/2015/nov/02/investigatory-powers-bill-snoopers-charter-will-remain-firmly-in-place [https://perma.cc/NZ86-AURW]; *see generally* Investigatory Powers Act 2016, c. 25 (UK).

10. Brian Wheeler, *Theresa May: We Need to Collect Communications Data 'Haystack'*, BBC (Oct. 16, 2014), http://www.bbc.com/news/uk-politics-29642607 [https://perma.cc/YS65-Q8DX]. Theresa May did not use this quote in direct reference to the Investigatory Powers Act (IP Act). *See id.* Rather, this quotation was used when she defended and advocated for surveillance policies. *See id.*

11. *See Royal Assent*, UK PARLIAMENT, http://www.parliament.uk/about/how/laws/passage-bill/lords/lrds-royal-assent/ (last visited Sept. 10, 2017) (royal assent is a formality whereby the Queen assents to a bill that has been passed by the U.K. Parliament) [https://perma.cc/A9US-SQN9].

12. Investigatory Powers Act 2016, c. 25, pmbl. (UK).

13. *See* Andrew Griffin, *Investigatory Powers Act Goes Into Force, Putting UK Citizens Under Intense New Spying Regime*, INDEPENDENT (Dec. 31, 2016), http://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-act-bill-snoopers-charter-spying-law-powers-theresa-may-a7503616.html [https://perma.cc/PE7Z-BWSL].

14. Julian Huppert, *The UK's Investigatory Powers Bill Is About to Become Law – Here's Why That Should Terrify Us*, OPEN DEMOCRACY (Oct. 17, 2016), https://www.opendemocracy.net/digitaliberties/julian-huppert/uk-investigatory-powers-bill-becomes-law-terrify-us [https://perma.cc/P5JB-6GJP].

15. *See* Robin Simcox, *Theresa May Can't Let Privacy Campaigners Get in The Way of Keeping Britain Safe*, TELEGRAPH (Oct. 11, 2016), http://www.telegraph.co.uk/news/2016/10/11/theresa-may-cant-let-privacy-campaigners-get-in-the-way-of-keepi/ [https://perma.cc/JS2U-DR9C].

16. *See* Joined Cases C-293/12 & C-594/12, Digital Rights Ireland v. Minister for Commc'ns, Marine and Natural Resources, Kärntner Landesregierung, 2014 E.C.R. I-238, ¶ 1; *see also* Owen Bowcott, *MP Calls for Limit on UK Surveillance Powers as EU Test Case Opens*, GUARDIAN (Apr. 12, 2016), https://www.theguardian.com/world/2016/apr/12/mp-david-davis-calls-limit-uk-surveillance-powers-european-court-justice (describing that two U.K. Members of Parliament (MP) are urging the Court of Justice of the European Union (CJEU) to stand by its judgment in *Digital Rights Ireland*) [https://perma.cc/FZE5-42PR].

In *Digital Rights Ireland*, the CJEU invalidated the E.U. Data Retention Directive[17]—a mandate effectively forcing telecommunications providers in the European Union to retain individuals' metadata—because it unjustifiably interfered with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFR).[18] The CJEU found the Directive's data retention mandate particularly problematic because it lacked sufficient safeguards and created too great a possibility that retained data could be used to draw infallible inferences regarding the most delicate parts of an individual's life.[19]

Critics of the IP Act adopted a similar sentiment to that of the CJEU in *Digital Rights Ireland*—the IP Act, like the Data Retention Directive, poses too great a risk to individual privacy rights.[20] Though many of the powers created by the IP Act are controversial,[21] this Note specifically addresses the IP Act's bulk acquisition warrant provisions. Bulk acquisition warrants permit authorized public authorities to access, in the aggregate, "the 'who', 'where', 'when', 'how' and 'with whom'" of retained metadata upon meeting certain conditions.[22] These conditions are overly broad and

17. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105/54) [hereinafter Data Retention Directive].

18. *See Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 68; *see also* Charter of Fundamental Rights of the European Union, pmbl., Oct. 26, 2012, 2012 O.J. (C 326/391) [hereinafter The CFR].

19. *See Digital Rights Ireland*, 2014 E.C.R. I-238, ¶¶ 26, 27, 54. For example, a former MP—Julian Huppert—warned that the Act creates a database that has the capability of showing that a person went to an abortion website or a marriage guidance website. *See* Jill Lawless, *U.K. Passes New Spy Bill—Now, Authorities Can See Internet Data of Entire Country*, STAR (Nov. 26, 2016), https://www.thestar.com/news/world/2016/11/26/uk-passes-snooping-law-now-residents-can-kiss-their-internet-privacy-goodbye.html [https://perma.cc/24G4-DWD6].

20. *See* Owen Bowcott, *Investigatory Powers Bill Not Fit for Purpose, Say 200 Senior Lawyers*, GUARDIAN (Mar. 14, 2016), https://www.theguardian.com/world/2016/mar/14/investigatory-powers-bill-not-fit-for-purpose-say-200-senior-lawyers (noting that former judges, law professors, senior lawyers, a U.N. special rapporteur, and privacy protection groups have articulated opposition to the IP Act) [https://perma.cc/H5BR-96MN]; Lawless, *supra* note 19.

21. *See* Andrew Griffin, *Investigatory Powers Bill Officially Passes into Law, Giving Britain the 'Most Extreme Spying Powers Ever Seen'*, INDEPENDENT (Nov. 29, 2016), http://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-bill-snoopers-charter-passed-royal-assent-spying-surveillance-a7445276.html (describing the opposition to the IP Act and other surveillance powers that the IP Act creates) [https://perma.cc/F5BD-67K9].

22. *Bulk Data*, SECURITY SERV. MI5, https://www.mi5.gov.uk/bulk-data (last visited Sept. 10, 2017) [https://perma.cc/D66T-G3JJ].

lack sufficient safeguards to protect fundamental rights to privacy. The United Kingdom should amend the IP Act and develop more exacting requirements before an intelligence agency may obtain a bulk acquisition warrant, because the IP Act's current framework abrogates the rights preserved in Articles 7 and 8 of the CFR.

Part I of this Note provides a background of the U.K. and E.U. legal framework relating to surveillance powers and its confrontation with the CFR. Part II examines how the IP Act's provisions governing bulk acquisition warrants unjustifiably interfere with Articles 7 and 8 of the CFR. Additionally, Part II proposes revisions to these provisions to balance the needs of U.K. intelligence agencies with the rights guaranteed and preserved in the CFR. Lastly, this Note briefly concludes and explains why the United Kingdom should still amend the IP Act even with the United Kingdom's announcement to leave the European Union.[23]

I. Background

A. *An Early History of Surveillance Legislation: 1984–2005*

The development of data protection laws has contemporaneously accompanied the rapid evolution in digital technology and Internet use.[24] In the early 1970s, during the Internet's incipiency, European states began experimenting with domestic data protection legislation.[25] Shortly thereafter, these states' domestic data laws conflicted with one another.[26] This lack of uniformity prompted an independent international organization—the Organization for Economic Cooperation and Development (OECD)—to recommend data privacy principles in hopes that countries would uniformly adopt them.[27] Because the OECD principles were

23. Central to this Note's critique of the IP Act is the Charter of Fundamental Rights for the European Union (CFR) and precedent provided by the CJEU. This Note was written shortly after the U.K. referendum to withdraw from the European Union. Given the uncertainty regarding Brexit's impact on the U.K.'s economic, political, and legal landscape, this Note analyzes the IP Act under the current E.U. human rights regime and acknowledges that the arguments herein may be negated by the future actions of the United Kingdom.

24. *See* Peter Hustinex, *Protection of Personal Data in a Digitalized World*, 82 L'Observateur de Bruxelles 1, 1–3, https://issuu.com/deboeck/docs/obxl_82 [https://perma.cc/LZ8Y-9G2M].

25. *See* Orla Lynskey, The Foundations of EU Data Protection Law, 47 (2015) (describing that the German state of Hesse, Sweden, and France were among the first countries to introduce data legislation).

26. *See id.*

27. *See* Peter Mei, The EC Proposed Data Protection Law, 25 L. & Pol'y Int'l Bus. 305, 305–08 (1993).

merely persuasive, the United Kingdom, as well as other E.U. member states, continued to enact independent domestic data legislation until the E.U. Parliament made its first harmonization effort in 1995.[28] First, this Note discusses the U.K. Telecommunications Act 1984—an important piece of data legislation that preceded the E.U. harmonization measures. Second, this Note discusses three E.U. directives related to data access and data retention, which attempted to homogenize data laws in the European Union.

1. U.K. Data Legislation Related to Data Access and Retention

The U.K.'s Telecommunications Act 1984, *inter alia*, sought to privatize British telecommunications and deregulate the U.K. telecommunications market.[29] Yet, one of the more subtle provisions of the Telecommunications Act—Section 94—created a broad power that authorized any secretary of state[30] to compel a telecommunications provider to both retain and provide an intelligence agency access to certain data within the provider's network if the secretary of state, first, consulted the provider, and second, believed such direction was "necessary in the interests of national security."[31] Thirty years later, in 2015, society learned that U.K. intelligence agencies used this power for more than a decade to acquire—in bulk—metadata that telecommunications providers were forced to retain.[32]

To utilize this surreptitious power, a secretary of state only needs to believe that the direction given to the telecommunications pro-

28. *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) [hereinafter Data Protection Directive]. The Organization for Economic Cooperation and Development principles were persuasive and served an influential role in shaping E.U. data privacy directives. *See generally* Ariel E. Wade, Note, *A New Age of Privacy Protection: A Proposal for An International Personal Data Privacy Treaty*, 42 Geo. Wash. Int'l L. Rev. 659, 668–69 (2010) (providing background about the evolution of the European Union's data privacy protection).

29. *See* Telecommunications Act 1984, c. 12, pmbl. (Eng.).

30. U.K. secretaries of state are cabinet members that head various government departments. *See Secretary of State*, Parliament.uk, http://www.parliament.uk/site-information/glossary/secretary-of-state/ (last visited Sept. 10, 2017) [https://perma.cc/Z5PL-4PFD]. There are at least fifteen secretaries that head departments ranging from education to defense. *Her Majesty's Government*, Parliament.uk, http://www.parliament.uk/mps-lords-and-offices/government-and-opposition1/her-majestys-government/ (last visited Sept. 10, 2017) [https://perma.cc/7XQQ-6AM8].

31. Telecommunications Act 1984, § 94(1)–(2) (such a direction may include turning over retained data).

32. Alan Travis et al., *Theresa May Unveils UK Surveillance Measures in Wake of Snowden Claims*, Guardian (Nov. 4, 2015), https://www.theguardian.com/world/2015/nov/04/theresa-may-surveillance-measures-edward-snowden [https://perma.cc/B5CK-25CG].

vider is proportionate to the goal sought to be achieved.[33] Though nothing in Section 94 prevents a provider from contesting the direction with the relevant secretary of state, the provider must comply if given the direction.[34] In the event that a secretary of state gives one or more of these directions to a telecommunications provider, Section 94 instructs the secretary of state to inform the U.K. Parliament of each direction given; however, a caveat in the Act allows the secretary of state to circumvent this step and to prevent a telecommunications provider from disclosing the direction if the secretary of state believes that disclosure would be against the interests of national security.[35]

This expansive power did not receive significant scrutiny until 2016, when the U.K.'s Interception of Communications Commissioner, Stanley Burnton, provided a report to the prime minister about the application of Section 94.[36] Commissioner Burnton criticized Section 94 as a statutory secrecy provision that lacked independent oversight and expiration dates on directions.[37] Further, his analysis highlighted that the bulk acquisition powers in the Telecommunications Act also exist in a separate, more transparent piece of U.K. legislation—the Regulation of Investigatory Powers Act 2000 (RIPA).[38] Notwithstanding this symmetric power, Burnton revealed that the United Kingdom preferred to collect data under Section 94 for at least two reasons.[39] First, retention notices lasted indefinitely under Section 94 of the Telecommunications Act, while retention notices under RIPA were subject to

33. *See* Telecommunications Act 1984, § 94(2). The term "direction" is used in the statute as a command given by the secretary of state. *See id.*

34. *See id.* § 94(3).

35. *See id.* § 94(4)–(5).

36. *See generally* STANLEY BURNTON, REPORT OF THE INTERCEPTION OF COMMUNICATIONS COMMISSIONER: REVIEW OF DIRECTIONS GIVEN UNDER SECTION 94 OF THE TELECOMMUNICATIONS ACT 1984 (2016). The Interception of Communications Commissioner (ICC) was created by the U.K.'s Regulation of Investigatory Powers Act (RIPA) to oversee specified exercises and performances of U.K. officials. Regulation of Investigatory Powers Act 2000, c. 23, § 57(1)–(2) (UK) [hereinafter RIPA]. Per the prime minister's 2015 request, Commissioner Burnton provided a report about the Telecommunications Act. *See* BURNTON, *supra* note 36 (stating the purpose of the report in a letter to the prime minister of the United Kingdom).

37. *See* BURNTON, *supra* note 36, ¶¶ 4.8, 4.10, 4.14–4.17.

38. *See id.* ¶ 8.19; RIPA, *supra* note 36, § 22. A designated person under § 22(2) of RIPA may obtain retained data from a telecommunications provider if he finds it necessary on one of the following grounds: in the interests of national security or public safety, for preventing or detecting crime, for protecting public health, for a charge payable to a governmental department, for preventing serious death or injury, or for an order made by the secretary of state. *See* RIPA, *supra* note 36, § 22.

39. *See* BURNTON, *supra* note 36, ¶¶ 8.20–8.21.

monthly renewal.[40] Second, Section 94 directions did not need to be presented to the U.K. Parliament and contained fewer procedural hurdles.[41]

Later in December 2016, the Investigatory Powers Tribunal (IPT) corroborated Burnton's findings in *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*.[42] The IPT was created by RIPA and is the only court permitted to hear complaints against U.K. intelligence agencies.[43] It held that U.K. intelligence agencies used Section 94 to unlawfully collect bulk data for at least seventeen years by concealing surveillance activities and failing to have proper oversight.[44] Further, the IPT found that GCHQ and MI5 each used Section 94, respectively since 1998 and 2005, to collect and acquire bulk data.[45] Yet, the secretary of state did not disclose any Section 94 direction to Parliament until November 2015.[46] Today, proponents of the IP Act point to the Telecommunications Act and RIPA as justifications for the IP Act's bulk acquisition powers.[47]

2. E.U. Directives Related to Data Access and Retention

In 1995, approximately ten years after the United Kingdom enacted the Telecommunications Act, the E.U. Parliament passed the Data Protection Directive, the first E.U. directive and harmonization effort regarding data privacy laws.[48] Among other things,

40. *See id.* ¶ 8.20

41. *See id.* ¶ 8.21. On the other hand, RIPA authorizations were required to be granted in a manner that produced a record, and required the authorization to specify the purpose and data to be obtained. *See* RIPA, *supra* note 36, § 23.

42. Privacy Int'l v. Sec'y of State for Foreign and Commonwealth Affairs, Case No. IPT/15/110/CH, Judgment (July 26–29, 2016), http://www.ipt-uk.com/docs/Bulk_Data_Judgment.pdf [https://perma.cc/G3GL-8QG7].

43. *See* Alan Travis, *UK Security Agencies Unlawfully Collected Data for 17 Years, Court Rules*, Guardian (Oct. 17, 2016), https://www.theguardian.com/world/2016/oct/17/uk-security-agencies-unlawfully-collected-data-for-decade [https://perma.cc/3UVU-TP6B].

44. Privacy International, Case No. IPT/15/110/CH, ¶¶ 10–15, 84 (noting that GCHQ primarily used Section 94 beginning in 2001).

45. *Id.* ¶ 10.

46. *Id.* ¶ 14.

47. Gov't of United Kingdom, Operational Case for Bulk Powers 8, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf (last visited Sept. 10, 2017) (justifying the analogous powers in the IP Act because they already existed in past legislation) [https://perma.cc/9DCQ-SVK7].

48. Data Protection Directive, *supra* note 28; *see* Lynskey, *supra* note 25, at 4. Directives are E.U. parliamentary legal instruments that compel member states to achieve a certain end through whatever means the member states deems appropriate. *See European Union Directives*, EUR-Lex, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14527 (last visited Sept. 10, 2017) [https://perma.cc/KSM9-59Z4]. Directives

the Directive seeks to provide a high level of protection for individuals' data and to protect privacy rights.[49] To accomplish these goals it imposes the following: (1) limitations on the extent of data processing, and (2) procedural safeguards concerning when personal data processing is legitimate.[50] However, the Directive permissively allows member states to inhibit these limitations and safeguards when necessary to ensure national security, defense, or public security.[51] Outside of this narrow exception, Article 22 of this Directive requires E.U. states to provide citizens a judicial remedy for any rights guaranteed by the legislation in question.[52] Though the General Data Protection Regulation will supersede the Data Protection Directive in May 2018, the latter played a significant role in shaping ensuing E.U. data legislation.[53]

For example, in 2002, the European Union enacted the E-Privacy Directive to both reaffirm the rights to privacy protected in the Data Protection Directive and to ensure that E.U. legislation stayed current with the rapid advancements in digital technology.[54] Article 5 of the E-Privacy Directive contributed to this goal by requiring member states to enact laws guaranteeing the confidentiality of electronic communications.[55] In order for member states to comply, the Directive instructs prohibitions on the storage, interception, and surveillance of communications data.[56] How-

---

are not self-executing and member states typically inject the directive's goal into domestic legislation to comply with the directive's mandate. *See id.*

49. *See* Data Protection Directive, *supra* note 28, pmbl., ¶ 10.

50. *See id.* art. 6–7. Article 6 requires that the data are processed fairly and lawfully, for unambiguous purposes and legitimate purposes, reasonable in relation to the purposes for which they were collected, accurate and kept up to date, and preserved for no longer than necessary to achieve the purposes for which the data were collected. *Id.* art. 6(1). The limitations regarding when data processing is legitimate is not pertinent to this Note. It is sufficient to understand that conditions exist to provide privacy protections. *See id.* art. 7.

51. *See id.* art. 13(1).

52. *See id.* art. 22.

53. *See* Commission Regulation 2016/679 of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, 86, ¶¶ 3, 9, 171 (E.U.) [hereinafter GDPR]; *GDPR Key Changes*, EUGDPR, http://www.eugdpr.org/key-changes.html (last visited Sept. 10, 2017) (providing a summary of the GDPR's main provisions that seek to protect E.U. citizens' data) [https://perma.cc/M4RE-NL2M].

54. *See, e.g.*, 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), 2003 O.J. (L 201), pmbl., ¶¶ 1–5 [hereinafter E-Privacy Directive].

55. *See id.* art. 5(1).

56. *See id.*

ever, like the Data Protection Directive before it, the E-Privacy Directive allows member states to limit the scope and obligations of the Directive when necessary to safeguard national security, defense, or public security.[57] Importantly, the E-Privacy Directive sought to bring data protection principles in line with Articles 7 and 8 of the CFR, just two years after the CFR's proclamation.[58]

B. *Statutory Human Rights Framework: The Charter of Fundamental Rights of the European Union*

The CFR is a comprehensive human rights framework encompassing the rights and principles in the European Convention on Human Rights and the judgments of both the CJEU and European Court of Human Rights.[59] Though the CFR's initial proclamation occurred in 2000, it only became legally binding on the European Union in 2009 through the Treaty of Lisbon.[60] Articles 7 and 8 of the CFR are pertinent to this Note because of the CJEU's recent judgments about surveillance legislation in the European Union and United Kingdom.[61] Article 7 sets out a general right to privacy while Article 8 provides the right to data protection.[62] These rights share a close relationship in the context of surveillance laws, and the CJEU often examines interferences with these rights together.[63] Though the CFR now holds treaty status, its applicability and scope to E.U. member states is limited in three ways.[64]

First, the CFR only applies to member states when they are "implementing EU law."[65] The exact breadth of this phrase is not entirely clear, but some scholars interpreting recent CJEU deci-

57. *See id.* art. 15(1).

58. *See id.* pmbl., ¶ 2; The CFR, *supra* note 18.

59. *See* The CFR, *supra* note 18, pmbl.

60. *See* Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, art. 6(1), Dec. 13, 2007, O.J. (C 306), art. 6(1) [hereinafter Treaty of Lisbon]; *Fact Sheets on the European Union: The Charter of Fundamental Rights*, EUR. PARLIAMENT, http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.1.6.html (last visited Sept. 10, 2017) [https://perma.cc/UKB2-DJCR].

61. *See, e.g.*, *Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 16(2)(ii).

62. *See* The CFR, *supra* note 18, art. 7–8. Article 7 provides that "[e]veryone has the right to respect for his or her private and family life, home and communications." *Id.* art. 7. Article 8 provides in pertinent part that "[e]veryone has the right to the protection of personal data concerning him or her" and that "[s]uch data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law." *Id.* art. 8.

63. *See, e.g.*, *Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 26; Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR v. Land Hessen, 2010 E.C.R. 662 (Nov. 9, 2010).

64. *See* Treaty of Lisbon, *supra* note 60 (making the CFR legally binding); The CFR, *supra* note 18.

65. The CFR, *supra* note 18, art. 51(1).

sions believe that the phrase broadly encompasses laws that have a sufficient connection to E.U. law.[66]

Second, and specifically related to the United Kingdom, is the unclear limitation imposed by Protocol 30 of the Treaty of Lisbon.[67] Protocol 30 states in pertinent part: "[t]he [CFR] does not extend the ability of the [CJEU], or any court . . . of the United Kingdom, to find that the laws . . . of the United Kingdom are inconsistent with the fundamental rights, freedoms and principles that it reaffirms."[68] Despite this seemingly unambiguous language, many experts agree that Protocol 30 is not an opt-out to the CFR, but rather is a limiting mechanism that reaffirms the existing CFR rights and prevents rights yet to come from becoming automatically binding on the United Kingdom.[69]

Third, the rights in the CFR are qualified.[70] Article 52(1) of the CFR allows member states to limit rights mentioned therein only if certain prerequisites are met. It provides:

> Any limitation . . . 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.[71]

The principle of proportionality, in relation to the CFR, requires a judicial or administrative body to ensure that the goals of a legislative act are legitimate and interfere no more than necessary with

---

66. *See* Richard Gordon qc & Rowena Moffatt, EU Law in Judicial Review 202 (Oxford Univ. Press 2d ed. 2014). Two scholars represent that "implementing E.U. law" is synonymous with acting within the scope of E.U. law. In pertinent part, they stated:

> [A] national measure may fall within the scope of EU law where it is taken pursuant to a general requirement of EU Law since the loyalty clause in Article 4(3) [of the Treaty on European Union] requires Member States to 'take any appropriate measure . . . to ensure fulfilment of obligations arising out of the Treaties . . . .'

Id. at 206.

67. Protocol 30 on the Application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom, Dec. 17, 2007, 2007 O.J. (C 306) 156 [hereinafter Protocol 30].

68. *Id.*

69. In 2014, the U.K.'s House of Commons European Scrutiny Committee aggregated the opinions of several experts and all concluded that Protocol 30 was not an opt-out to the CFR. *See* European Scrutiny Comm., The Application of the EU Charter of Fundamental Rights in the U.K.: A State of Confusion 29 (2014). A handful of these experts noted that even if Protocol 30 was an opt-out, it would still be applicable to the United Kingdom under Article 6(3) of the Treaty on the European Union because the Charter consists of general principles of E.U. law. *See id.* at 31.

70. *See* The CFR, *supra* note 18, art. 52(1).

71. *Id.* (emphasis added).

the various fundamental rights articulated in the CFR.[72] In striking down the Data Retention Directive, the CJEU applied an extensive proportionality analysis.[73] The CJEU's proportionality analysis, discussed in more detail below, is pertinent to the legality of the IP Act.

C. *Modern History of Surveillance Legislation: 2006–2017*

1. The Data Retention Directive and *Digital Rights Ireland*

In 2006, the European Parliament passed the Data Retention Directive, likely to better equip member states' intelligence agencies after the tragic incidences of terrorism in Spain and England.[74] The Directive required member states to regulate telecommunications providers by requiring providers to retain users' traffic and location data, or in more colloquial terms, metadata.[75] Even though the Directive did not permit retention of the content of a communication,[76] the CJEU eventually declared it invalid in *Digital Rights Ireland*.[77] *Digital Rights Ireland* reached the CJEU after two E.U. countries referred a question to the CJEU regarding the Data Retention Directive's compatibility with Articles 7 and 8 of the CFR.[78] Ultimately, the CJEU declared the Directive invalid because it unjustifiably interfered with Articles 7 and 8 of the CFR.[79]

The CJEU conducted its analysis in *Digital Rights Ireland* using a two-pronged approach.[80] First, the CJEU sought to determine whether the Data Retention Directive *interfered* with individual rights as preserved in the CFR.[81] Second, because the Directive

72. *See* Gordon & Moffatt, *supra* note 66, at 343.

73. *See infra* Section II.C.1.

74. Data Retention Directive, *supra* note 17; *see Spain Train Bombings Fast Facts*, CNN Libr. (Mar. 5, 2017), http://www.cnn.com/2013/11/04/world/europe/spain-train-bombings-fast-facts/ [https://perma.cc/P3DB-3H95]; *July 7 2005 London Bombings Fast Facts*, CNN Libr. (June 29, 2017), http://www.cnn.com/2013/11/06/world/europe/july-7-2005-london-bombings-fast-facts/ [https://perma.cc/89DL-YBDZ]; *see also* Fabbrini, *supra* note 2, at 85 (commenting that the Data Retention Directive was pushed through the legislative process after the 2005 London bombings).

75. *See* Data Retention Directive, *supra* note 17, art. 2(2)(a) (data to identify the user); Fabbrini, *supra* note 2.

76. *See* Data Retention Directive, *supra* note 17, art. 5(2).

77. *Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 71.

78. The CJEU answered the courts' questions under the preliminary reference procedure—a mechanism allowing the highest courts in E.U. member states to refer inquiries regarding the validity of E.U. directives to the CJEU. *See* Fabbrini, *supra* note 2, at 76–78.

79. *Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 69.

80. *See id.*

81. *See id.* ¶¶ 32–37.

infringed on these rights, the CJEU examined whether such interference was *justified*.[82]

First, the CJEU held that the Directive seriously interfered with Article 7's general right to privacy and with Article 8's right to data protection because metadata does not merely record the who, where, when, and how of a communication.[83] Rather, it documents a history about individuals that "*may* allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained."[84] In considering this conjectural risk, the CJEU rebuffed any notion that the interference with the right to privacy required a showing that retained data was sensitive or disconcerting to the individual.[85]

Second, the CJEU used a separate two-part inquiry to determine whether this interference was justified under Article 52(1) of the CFR's *proportionality principle*.[86] The first inquiry asked whether the Directive satisfied an objective of general interest.[87] The CJEU found that the Directive satisfied this prong because fighting serious crime and terrorism is an established objective of general interest.[88] The second inquiry analyzed whether the Directive exceeded the limits of what is appropriate and necessary to accomplish its objectives.[89] The CJEU ultimately held that the Directive failed this prong because the interferences with the CFR lacked narrow tailoring and instead interfered with virtually all individuals in the European Union.[90]

The CJEU extensively supported its holding with strong language. For example, it stated that interferences with privacy must be accompanied by "*clear and precise rules* . . . so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access to that data."[91] Contrary to this principle, the Directive applied to individuals utterly unconnected with a crime, failed to place sufficient limits on the authorities' use of

82. *See id.* ¶¶ 38–46.
83. *See id.* ¶¶ 26, 69.
84. *Id.* ¶ 27 (emphasis added).
85. *Id.* ¶ 33.
86. *Id.* ¶ 20; *see supra* note 71 and accompanying text.
87. *Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 41.
88. *Id.*
89. *See id.* ¶ 46.
90. *Id.* ¶¶ 58–60. For example, the Directive compelled data retention for all users of Internet communications and telephony with no regard to whether that retention was necessary to combat serious crime or terrorism. *Id.*
91. *Id.* ¶ 54 (emphasis added).

retained data, and omitted a provision making the use of retained data contingent upon judicial or administrative review.[92]

2. The U.K.'s Response to *Digital Rights Ireland*: The Data Retention and Investigatory Powers Act

Despite the result in *Digital Rights Ireland*, the judgment failed to proscribe member states from continuing to use their present data retention laws or from enacting new data retention laws to comply with human rights principles.[93] Accordingly, the United Kingdom scrambled to preserve its surveillance powers and quickly enacted the Data Retention and Investigatory Powers Act (DRIPA) in 2014.[94] DRIPA empowered the secretary of state to issue retention notices, which compelled telecommunications providers to retain metadata for any purpose falling under RIPA Section 22(2).[95] Though DRIPA addressed some of the CJEU's concerns in *Digital Rights Ireland*, such as providing a maximum retention period of one year[96] and oversight by an independent reviewer of terrorism,[97] it was a short term solution given its expiration date of December 31, 2016.[98] Notwithstanding these corrections, MPs challenged DRIPA's validity in the U.K. High Court of Justice (HCJ) based on the CJEU's judgment in *Digital Rights Ireland*.[99] Eventually, this challenge reached the CJEU in *Tele 2 Sverige AB v. Post-och Telestyrelsen*.[100]

---

92. *Id.* ¶¶ 55–62.

93. *See* Lawrence Drewry, *Crimes Without Culprits: Why the European Union Needs Data Retention, And How It Can Be Balanced with the Right to Privacy*, 33 Wis. Int'l L.J. 728, 735 (2015).

94. *See* Data Retention and Investigatory Powers Act 2014, c. 27, pmbl. (UK) (establishing that the Act is "in consequence of a declaration of invalidity made by the Court of Justice of the European Union in relation to Directive 2006/24/EC") [hereinafter DRIPA].

95. *See id.* § 1(1); *see also* RIPA, *supra* note 36, § 22(2).

96. *See* DRIPA, *supra* note 94, § 1(5).

97. *See id.* § 7(1)–(8). The independent reviewer of terrorism legislation is an official appointed under the U.K. Terrorism Act 2006 § 36(1) who periodically reviews and provides a report to the prime minister regarding the U.K.'s investigatory powers, the threats challenging the United Kingdom, and the functions needed to overcome those threats. *See id.*

98. *See id.* § 8(3).

99. *See* Davis v. Sec'y of State for the Home Dep't [2015] EWHC (Admin) 2092 [17]–[19] (Eng.). The High Court of Justice (HCJ) is a U.K. court that handles civil matters. *See The High Court*, Brief, http://www.inbrief.co.uk/legal-system/high-court/ (last visited Sept. 10, 2017) [https://perma.cc/86KH-CQSB]. Appeals from the HCJ are directed to the U.K. Court of Appeal (COA). *See id.*

100. *See* Joined Cases C-203/15 & C-698/15, Tele2 Sverige AB v. Post-och Telestyrelsen, 2016 E.C.R. 970, ¶¶ 1–2.

3. The Challenge to DRIPA: *Davis* and *Tele2 Sverige AB*

In 2015, the HCJ held in *Davis v. Secretary of State for the Home Department* that DRIPA is inconsistent with E.U. law.[101] The HCJ noted that *Digital Rights Ireland* required more than just mandatory limitations on data retention; it also required data access regimes to contain ample safeguards that prevent unlawful access to such data.[102] To the HCJ, *Digital Rights Ireland* imposed mandatory requirements for data access legislation including (1) the existence of specific rules and safeguards to protect data from abuses and unlawful access, (2) an access regime that is limited to "preventing and detecting precisely defined serious offen[s]es," and (3) administrative or judicial review prior to any data access.[103] Subsequently, the U.K. government appealed this decision to the U.K. Court of Appeal (COA).[104]

The COA disagreed that *Digital Rights Ireland* imposed mandatory requirements and opined that the HCJ extended the CJEU's language beyond a fair reading of the judgment in *Davis*.[105] However, the COA refused to provide judgment and instead referred the question to the CJEU on whether the CJEU intended to articulate mandatory requirements for member states' domestic data legislation.[106] Notably, in the time period between the COA's referral and the CJEU's eventual answer in *Tele2 Sverige AB*, the IP Act became official law.[107]

In answering the COA's question in *Tele2 Sverige AB*, the CJEU held that *Digital Rights Ireland* imposed mandatory requirements with unambiguous language.[108] First, data access *must* correspond to one of the objectives articulated in Article 15(1) of the E-Privacy Directive[109] because access to personal data interferes with that

101. *See Davis*, [2015] EWHC 2092 [62], [122].

102. *See id.* [85]–[89].

103. *Id.* [91].

104. *See* Sec'y of State for the Home Dep't v. Davis [2015] EWCA (Civ) 1185 [2] (Eng.).

105. *See id.* [74]–[79] (noting that if the CJEU wished to create mandatory requirements, it would have used explicit language to do so).

106. *See id.* [118].

107. *See generally* Investigatory Powers Act 2016, c. 25 (UK); Oliver Murphy, *Investigatory Powers Act Gets Royal Assent*, Reynolds Porter Chamberlain LLP (Dec. 2, 2016), https://www.rpc.co.uk/perspectives/data-and-privacy/investigatory-powers-act-gets-royal-assent [https://perma.cc/U8ZQ-QF35].

108. *See Tele2 Sverige AB*, 2016 E.C.R. 970, ¶ 53. *Tele2 Sverige AB* answered two referred questions, one from the Stockholm Administrative Court of Appeal and one from the U.K. Court of Appeal. *See id.* ¶ 2. Stockholm's question primarily concerned the legality of "general and indiscriminate *retention* of . . . data." *Id.* ¶ 62.

109. *See supra* note 57 and accompanying text.

Directive's confidentiality of communications principle.[110] Specifically, in regards to preventing, investigating, detecting, or prosecuting a criminal offense, access is *only* permitted when the crime is a *serious crime*.[111] The CJEU did not provide a definition or criteria for what constitutes a serious crime, but rather left that task to member states.[112]

Second, to comply with the proportionality principle, access to retained data *must* not exceed what is strictly necessary.[113] Legislation only complies with this requirement if it establishes "clear and precise rules indicating in what circumstances and under which [specific[114]] conditions the providers of electronic communications services must grant the competent national authorities access to the data."[115] The conditions referred to in the preceding sentence must be substantive, procedural, and based on objective criteria.[116]

Third, after an individual's data has been accessed, the national authorities are *required* to notify that individual immediately at the time when the notification will no longer jeopardize the government operation.[117] This requirement exists because Article 15(2) of the E-Privacy Directive, read in conjunction with Article 22 of the Data Protection Directive, creates a judicial remedy where an individual's rights have been infringed.[118] Without a notification, an individual would be unable to pursue a legal remedy.

Fourth, the CJEU stated that either a court or independent administrative body should—"*as a general rule*"—review access to retained data unless the urgency of a situation dictates otherwise.[119] Overall, the judgment provided clarity that indiscriminate

110. *See Tele2 Sverige AB*, 2016 E.C.R. 970, ¶ 115; *see also* E-Privacy Directive, *supra* note 54, art. 5 (confidentiality of communications principle).

111. *See Tele2 Sverige AB*, 2016 E.C.R. 970, ¶ 115 (emphasis added) (the phrase, "serious crime," is not defined in the opinion).

112. *See id.* ¶¶ 118–19.

113. *See id.* ¶ 116; *see also id.* ¶ 119 (noting that for matters involving serious crime, only data associated with the culprits may be accessed, while for matters involving national security, authorities may access individuals' data that fall outside those associated with the crime).

114. The CJEU clarified that merely listing the general conditions mentioned in Article 15(1) of the E-Privacy Directive will not satisfy this requirement. *See id.* ¶ 118. For example, listing "in the interests of national security," is a legitimate objective, but the rules and conditions must provide greater specificity. *See id.* ¶¶ 118–19.

115. *Id.* ¶ 117.

116. *See id.* ¶¶ 118–19.

117. *See id.* ¶ 121.

118. *See id.*

119. *See id.* ¶ 120 (emphasis added).

data retention is inconsistent with E.U. law and gave member states guidance about how to implement compliant surveillance legislation.[120] *Tele2 Sverige AB*'s impact on U.K. intelligence policy is not settled as U.K. courts and Parliament now seek to internalize and adapt to the judgment.[121] As for DRIPA, that Act has since expired and the U.K.'s IP Act 2016 is now the center of attention.[122]

D. *The U.K.'s Investigatory Powers Act 2016*

The United Kingdom enacted the IP Act into law in November 2016.[123] It became effective on January 1, 2017, immediately after DRIPA's expiration.[124] Part 6 of the IP Act governs bulk acquisition warrants.[125] These warrants compel mentioned telecommunications providers to disclose retained communications data to intelligence agencies as specified in the warrant.[126] However, because the existence of retained data presupposes data access, it is first necessary to understand the type of data to which these warrants provide access.[127]

Part 4 of the IP Act authorizes the secretary of state to require a telecommunications provider to retain communications data

120. *See* Allison Grande, *EU Data Retention Slam Offers Telecoms Cloudy Path Forward*, Law360 (Dec. 22, 2016), https://www-law360-com.gwlaw.idm.oclc.org/articles/876172/eu-data-retention-slam-offers-telecoms-cloudy-path-forward [https://perma.cc/EHJ6-G2BJ].

121. *See Tele2 Sverige AB*, 2016 E.C.R. 970, ¶¶ 124–25; Max Hill, *CJEU Judgment in Watson*, Terrorism Legislation Reviewer (Dec. 21, 2016), https://terrorismlegislationreviewer.independent.gov.uk/cjeu-judgment-in-watson/ [https://perma.cc/PAM5-C5FY].

122. *See* DRIPA, *supra* note 94, §8(3); Investigatory Powers Act 2016, c. 25, pmbl. (UK).

123. *See* Investigatory Powers Act, c. 25, pmbl. (UK).

124. *Id.*; Kevin Townsend, *EU Court Slaps Down UK's Investigatory Powers Act*, Securityweek (Dec. 22, 2016), http://www.securityweek.com/eu-court-slaps-down-uks-investigatory-powers-act [https://perma.cc/P2VD-HWCF]; Graham Smith, *The UK Investigatory Powers Act 2016 – What It Will Mean for Your Business*, Bird & Bird (Nov. 29, 2016), https://www.twobirds.com/en/news/articles/2016/uk/what-the-investigatory-powers-bill-would-mean-for-your-business [https://perma.cc/245S-4K3H].

125. *See* Investigatory Powers Act, c. 25, §§ 158–75 (UK).

126. *See id.* § 158(6) (UK); *see also* U.K. Parliament, Bulk Acquisition of Communications Data: Draft Code of Practice §§ 1.2, 4.1 (Feb. 2017), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/593750/IP_Act_-_Draft_BCD_code_of_practice_Feb2017_FINAL_WEB.pdf ("An application for a bulk acquisition warrant therefore may only be made by or on behalf of . . . [t]he Director General of the Security Service; [t]he Chief of the Secret Intelligence Service; or [t]he Director of [GCHQ].") [https://perma.cc/6SEU-PBZG].

127. It is worthwhile to mention that this Note does not analyze the validity of the IP Act's data retention regime. Some parts of the data retention regime seem eerily like the Data Retention Directive—struck down in *Digital Rights Ireland*—but at a minimum, the United Kingdom addressed some of the CJEU's concerns by making retention notices expire after one year and subjecting retention notices to mandatory judicial review. *See* Investigatory Powers Act 2016, c. 25 (UK), §§ 61–71.

through a retention notice.[128] Communications data is analogous to metadata and includes the communications' sender, recipient, time, length, method of sending, and location from which it was sent.[129] This also includes Internet connection records—a log of every IP address one has accessed in the past year.[130] To borrow another one of Prime Minister May's analogies, data retention under the IP Act is like an itemized phone bill that, *inter alia*, shows the time and duration of service usage, the amount of data uploaded or downloaded, and other related records.[131]

To acquire this retained data, intelligence agencies may submit an application to the secretary of state to obtain a bulk acquisition warrant.[132] If issued, these warrants compel mentioned telecommunications providers to disclose retained communications data to intelligence agencies.[133] Two features of these warrants deserve attention.

First, these warrants permit the *bulk* collection of metadata, as opposed to *targeted* collection of metadata, regarding a specific individual.[134] The United Kingdom rationalizes this feature because the popularity of Internet communications over time has reduced the effectiveness of traditional targeted acquisition warrants.[135] Accordingly, the United Kingdom believes that the bulk acquisition of data will allow intelligence agencies to sift through

128. *See id.* §§ 87–98.

129. *See id.* § 87(11) (a communication's content is not included in communications data).

130. U.K. Parliament, Investigatory Powers Bill Fact Sheet—Internet Connection Records, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473745/Factsheet-Internet_Connection_Records.pdf [https://perma.cc/2KHA-KML4].

131. *See* Madhumita Murgia, *Itemised Phone Logs Reveal Scary Personal Details About You, Study Finds*, Telegraph (May 17, 2016), http://www.telegraph.co.uk/technology/2016/05/17/itemised-phone-logs-reveal-scary-personal-details-about-you-stud/ [https://perma.cc/R3ZV-XRRS].

132. *See* Investigatory Powers Act 2016, c. 25 (U.K.), § 158.

133. *Id.* §§ 158(6)–(7).

134. *See id.*; *see also* Operational Case for Bulk Powers, *supra* note 47, ¶ 2.1.

135. Operational Case for Bulk Powers, *supra* note 47, ¶¶ 1.5–1.8. In 1995, less than one percent of the E.U. population used the Internet. *See* Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner, Outdoing Huxley: Forging a High Level of Data Protection for Europe in the Brave New Digital World, Address at Digital Enlightenment Forum (June 18, 2012), at 2. However, that percentage rose to approximately eighty percent of the E.U. population just twenty years later. *See Digital Economy and Society Statistics - Households and Individuals*, Eurostat: Stats. Explained, http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Main_statistical_findings (last visited Sept. 10, 2017) [https://perma.cc/W36K-7ECT].

an aggregation[136] of metadata, extract useful portions, and subsequently connect the dots to keep the United Kingdom safe from serious crime and terrorist attacks.[137] Second, these warrants permit access to an infinite amount of communications data because they are not constrained to a particular operation, thus extending access to future, not yet created, data.[138]

1. Procedure to Obtain a Bulk Acquisition Warrant

In order for an intelligence agency to obtain a bulk acquisition warrant, it must apply to the secretary of state.[139] The secretary of state may grant this request only if he concludes that the following five elements are satisfied.

First, according to Section 158(1)–(2), the secretary of state must conclude that the warrant is necessary (a) "in the interests of *national security*," (b) "for the purpose of preventing or detecting *serious crime*," or (c) "in the interests of the *economic well-being of the United Kingdom*" so long as that interest relates to the interests of national security.[140] Out of these italicized phrases, the IP Act only defines "serious crime."[141]

Second, the secretary of state must weigh whether the conduct authorized by the warrant is proportionate with the goal sought to be achieved.[142] The IP Act does not provide an indication of whether there are certain considerations, criteria, or principles that the secretary of state must refer to in making this assessment.[143] However, it is presumable that this proportionality assess-

136. Some commentators have noted that the collection of metadata may be more intrusive to privacy rights than targeted searches because metadata is "already categorised, which makes it much easier to aggregate and cross reference." Glyn Moody, *Why the Investigatory Powers Act is a Privacy Disaster Waiting to Happen,* Ars Techina UK (Nov. 17, 2016), https://arstechnica.co.uk/tech-policy/2016/11/investigatory-powers-act-privacy-disaster-waiting-to-happen/ [https://perma.cc/LCV9-9DF9].

137. *See* Operational Case for Bulk Powers, *supra* note 47, ¶ 1.7.

138. *See* Investigatory Powers Act 2016, c. 25 (UK), § 158(8); U.K. Parliament, Bulk Acquisition: Draft Code of Practice, § 3.4 (Autumn 2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557863/IP_Bill_-_Draft_Bulk_acquisition_code_of_practice.pdf [https://perma.cc/2YZD-FDRD].

139. *See* Investigatory Powers Act 2016, c. 25 (UK), § 158(1).

140. *Id.* § 158(1)–(2) (emphasis added).

141. *See id.* § 263(1). A "serious crime" under the IP Act is defined as an "offence, or one of the offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 18 . . . and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more," or where "the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose." *Id.*

142. *See id.* § 158(1)(b).

143. *See id.*

ment is consistent with the European Union's proportionality assessment and thus requires the secretary of state to consider whether the goals of the warrant are legitimate and interfere no more than necessary with the fundamental rights preserved in the CFR.[144]

Third, the secretary of state must consider that the intelligence agencies' operational purposes for both obtaining and examining the data are necessary—a requirement that seemingly exists to narrow an intelligence agency's use of the warrant.[145] However, the heads of intelligence agencies manage the comprehensive list of valid operational purposes and a secretary of state may approve new operational purposes so long as they are more specific than a regurgitation of the descriptions in Section 158(1)–(2).[146] Furthermore, this list is confidential and the Intelligence and Security Committee of Parliament—the oversight body—is only alerted of newly added operational purposes at the end of successive three-month periods.[147]

Fourth, the secretary of state must find that there are satisfactory arrangements to safeguard an individual's personal data.[148] For example, the extent of data disclosure to persons and the copying of data must be limited to what is necessary for the authorized purpose.[149]

Fifth, a judicial commissioner must approve of the issuance of the warrant—a step that one commentator characterizes as "double lock."[150] The reviewing Commissioner must, *inter alia*, conclude that the warrant is (a) "necessary in the interests of national security," "for the purpose of preventing or detecting serious crime," or "in the interests of the *economic well-being of the United Kingdom*" so long as the economic interest relates to an interest of national security; (b) the scope of the warrant is proportionate to its goals; and (c) that the specified operational purposes are or may be necessary, and the examination of such data is necessary.[151]

144. *See supra* note 72 and accompanying text.

145. *See* Investigatory Powers Act 2016, c. 25 (UK), § 158(1)(c).

146. *See id.* § 161; Operational Case for Bulk Powers, *supra* note 47, ¶ 6.12. Though a U.K. document professes that the list of operational purposes will contain "granular detail," the example purposes listed fall under broad umbrellas such as counter-terrorism, counter-proliferation, and addressing serious crime. Operational Case for Bulk Powers, *supra* note 47, ¶ 6.12.

147. *See* Investigatory Powers Act 2016, c. 25 (UK), § 142.

148. *See id.* § 158(1)(d).

149. *See id.* § 171(2).

150. *See id.* § 158(1)(e); Moody, *supra* note 136.

151. Investigatory Powers Act 2016, c. 25 (UK), §§ 158(1)–(2) (emphasis added).

II. Analysis

The United Kingdom enacted the IP Act nearly five years after Edward Snowden announced the invasiveness of U.K. intelligence agencies' practices.[152] Its bulk acquisition warrant regime is reminiscent of Orwellian interference, jeopardizing individuals' tranquility of mind through Big Brother-like oversight.[153] Even taking the justifications for bulk acquisition warrants as true—for instance, detecting and preventing terrorist attacks[154]—the IP Act must not be considered valid if its tremendous interferences with guaranteed rights in the CFR outweigh its utility. At the same time, the validity of the IP Act must not be viewed so narrowly that the resultant interpretation will condemn other objectives that the CFR seeks to promote. To achieve this balance, the United Kingdom should amend the IP Act and develop more exacting requirements before a secretary of state is able to issue a bulk acquisition warrant because the IP Act's current framework abrogates the rights preserved in Articles 7 and 8 of the CFR. In support of this proposition, this Note first, explains why the CFR is applicable to the United Kingdom; second, it demonstrates how the current articulation of the IP Act is incompatible with the CFR; and third, it develops a proposal to align the IP Act with the CFR.

A. *The Applicability of the Charter of Fundamental Rights to the IP Act*

Despite the ostensible impediments posed by Article 51(1) of the CFR and Protocol 30, the CFR is an appropriate legal instrument to analyze the IP Act given the CJEU's recent judgments in *Digital Rights Ireland* and *Tele2 Sverige AB*.[155] First, Article 51(1)'s ambigu-

152. *See id.*, pmbl.

153. Compare Ninety per cent of Brits Believe Government Surveillance Powers Contained in New Snoopers' Charter are not Acceptable, New Poll Finds, Liberty (June 5, 2016), https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/ninety-cent-brits-believe-government-surveillance-powers (finding that ninety percent of U.K. citizens do not approve of the surveillance powers within the Investigatory Powers Act), with Asa Bennett, Actually British Voters Don't Mind Mass Surveillance, Telegraph (Mar. 2, 2016), http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/12179248/Actually-British-voters-dont-mind-mass-surveillance.html (stating that approximately half of those surveyed support the expansion of U.K. surveillance powers). See also Eli R. Shindelman, Time for the Court to Become "Intimate" with Surveillance Technology, 52 B.C. L. Rev. 1909, 1932 n.230 (2011) (noting the term "Orwellian" derives from "George Orwell's novel [Nineteen Eighty-Four], where Big Brother, the dictator of the totalitarian state of Oceania, continuously monitors Oceania's inhabitants").

154. *See* Operational Case for Bulk Powers, *supra* note 47, ¶ 9.1 (noting that every major counter-terrorism operation involved bulk acquisitions powers over the last decade).

155. *See supra* notes 64–69 and accompanying text.

ous proposition that the CFR only applies to member states when they are "implementing E.U. law" may reasonably be interpreted to include situations when there is a sufficient connection to E.U. law.[156] The IP Act satisfies this connection to E.U. law because its origination is highly tied to the CJEU's invalidation of the Data Retention Directive in *Digital Rights Ireland*.[157] Even though DRIPA was the direct response to *Digital Rights Ireland*, that legislation was temporary from the outset.[158] Consequently, the United Kingdom enacted the IP Act, which integrated many of the CJEU's concerns regarding data access and retention regimes.[159] Additionally, both the IP Act and the judgment in *Digital Rights Ireland* seek to illuminate the degree of interference that data retention and data access legislation may have with rights to privacy.[160] Given the totality of the circumstances, the IP Act has the necessary connection to E.U. law to analyze its validity under the CFR.

Second, the effect of Protocol 30 is legally uncertain and should not inhibit the CFR's application to the IP Act for at least two reasons.[161] At a minimum, interpreting Protocol 30 as a complete opt-out may hinder the consistent application of the CFR across E.U. member states.[162] Further, even if Protocol 30 is interpreted as a complete opt-out, the CFR's value is not negated because the CFR holds equal weight to treaties.[163] Article 4(3) of the Treaty on European Union requires member states to ensure fulfillment of obligations arising out of the treaties.[164] To not give any weight to the CFR would contradict the Treaty on European Union.[165] Accordingly, the CFR is a proper legal instrument to analyze the IP Act.

---

156. *See supra* notes 64–69 and accompanying text.

157. *See* discussion *infra* Section II.C.

158. *See supra* note 98 and accompanying text.

159. *See* Investigatory Powers Act 2016, c. 25 (UK), pmbl. The Investigatory Powers Act, *inter alia*, added mandatory judicial review before a data retention notice may be issued and before a bulk acquisition warrant may be accessed. *See id.* §§ 89, 144.

160. *Id.* § 1; *Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 58.

161. *See* Protocol 30, *supra* note 67.

162. *See* The Application of the EU Charter of Fundamental Rights in the U.K.: A State of Confusion, *supra* note 69, ¶¶ 83–88.

163. *See id.* ¶ 146.

164. *See* Gordon & Moffatt, *supra* note 66, at 206.

165. *See id.*

B. *The Incompatibility Between the Charter of Fundamental Rights and the IP Act's Bulk Acquisition Warrant Provisions*

The IP Act's bulk acquisition warrant provisions, viewed in light of the CFR, are invalid because its data access regime's interference with the CFR is not justified under a proportionality analysis. The ensuing analysis applies the proportionality analysis the CJEU conducted in *Digital Rights Ireland* to the IP Act.[166] First, it discusses how the bulk acquisition warrant provisions interfere with Articles 7 and 8 of the CFR. Second, it discusses why this interference is not justified.

1. Interference Analysis

The IP Act's bulk acquisition warrant provisions interfere with Articles 7 and 8 of the CFR.[167] The United Kingdom already conceded that obtaining data via a bulk acquisition warrant would practically always interfere with individuals' right to privacy and communications.[168] This admission likely stems from *Digital Rights Ireland*, in which the CJEU indicated that Article 7 and Article 8 are delicate rights that are seemingly always interfered with within the context of *data retention* and subsequent data access.[169] Similarly, *bulk data access*, by its very definition, interferes with Article 8's right to the protection of personal data.[170]

However, the IP Act does not just interfere with the CFR because it permits data access—rather, it *seriously* interferes with the CFR because its procedural safeguards lack specificity and substance and fail to conform with *Digital Rights Ireland* and *Tele2 Sverige AB*'s mandatory requirements for surveillance laws.[171] For example, the IP Act does not define operative phrases like "in the interests of national security or [in the interests of] the economic well-being of the United Kingdom."[172] This interference is immensely serious because virtually any proffered reason fits under these operative phrases.

---

166. *See supra* Section II.C.1.

167. *See supra* note 62.

168. *See* BULK ACQUISITION: DRAFT CODE OF PRACTICE, *supra* note 138, § 3.8. This U.K. document did not refer explicitly to Articles 7 and 8 of the CFR, but rather referred to Article 8 of the European Convention on Human Rights. This right corresponds to the same right guaranteed by Article 7 of the CFR and was construed in the same manner as preserved in the European Convention on Human Rights.

169. *See Digital Rights Ireland*, 2014 E.C.R. I-238, ¶¶ 25–37.

170. *Id.* ¶¶ 35–36.

171. *See supra* Section II.C.1–2.

172. *See supra* notes 140–147.

Additionally, the IP Act's minimal threshold for the validation of new operational purposes recommended by an intelligence agency interferes with the CFR by providing lackluster assurances to individuals that their private communications will be protected.[173] Like in *Digital Rights Ireland*, this interference is serious because it is "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[174] This interference is magnified due to the recent judgment in *Privacy International*, in which the IPT found that U.K. intelligence agencies were surreptitiously using bulk acquisition powers to collect data about U.K. citizens.[175]

Moreover, the IP Act does not contain a provision guaranteeing that individuals will be notified after national authorities access their personal data at a time when the notification will not jeopardize the intelligence operation.[176] These fundamental omissions and overall lack of specificity in the IP Act make the existing procedural safeguards standardless, encourage unlawful access, and make the concerns of the CJEU more likely to come to fruition.[177]

2. Justification Analysis

The aforementioned interferences are not justified under Article 52(1) of the CFR because the bulk acquisition warrant provisions exceed what is necessary under the proportionality principle.[178] As the CJEU demonstrated in *Digital Rights Ireland*, this principle consists of two inquiries: (1) whether the legislation satisfies an objective of general interest, and (2) whether the legislation exceeds the limits of what is necessary to accomplish the legislation's objectives.[179]

The IP Act's bulk acquisition warrant provisions undoubtedly satisfy an objective of general interest because the provisions exist to help intelligence agencies fight terrorism and serious crime.[180] Quantifiably, the acquisition of communications data impacted

173. *See supra* notes 145–147.

174. *See Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 37.

175. *See* Privacy Int'l v. Sec'y of State for Foreign and Commonwealth Affairs, Case No. IPT/15/110/CH, Judgment, ¶¶ 10–15, 84 (July 29, 2016), http://www.ipt-uk.com/docs/Bulk_Data_Judgment.pdf [https://perma.cc/2RDG-GCG8].

176. *See* Investigatory Powers Act 2016, c. 25 (UK). *But see Tele2 Sverige AB*, 2016 E.C.R. 970, ¶ 121 (providing notification must occur at an appropriate time to individuals after their information has been accessed by authorities in the course of an investigation).

177. *See supra* note 19.

178. *See supra* notes 70–73.

179. *See supra* notes 86–89.

180. *Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 51.

every counter terrorism operation between 2004–2014 and also played a substantial role in thwarting offenders of serious crime.[181] The CJEU determined that both of these objectives constituted objectives of general interest in *Digital Rights Ireland* and there is no indication that this view is outdated.[182]

However, the IP Act's interference with the CFR is not justified because it exceeds the limits of what is strictly necessary to ensure national security interests and prevent serious crime.[183] Despite the importance of these objectives, they must not be given such extensive discretion to justify *any* interference with Article 7 and Article 8 of the CFR.[184] This effectively calls for a balancing between the severity of the interference and the objectives sought to be achieved.[185]

The failure to define operative phrases in the statute such as "in the interests of national security" and "economic well-being" creates over-breadth and risks expansive authority to collect data beyond the purported narrow parameters.[186] Though there may be some merit to a claim that the breadth of these definitions allows intelligence agencies to act flexibly and responsively, any claim that these definitions need to be left unbounded is specious. Otherwise, individuals would lack any reasonable expectation about the degree of interference with their guaranteed right to privacy.[187] As proposed later in this Note, a middle ground exists to balance the needs of intelligence agencies with individuals' fundamental rights to privacy.[188]

Additionally, the operative phrases in the IP Act need to be defined to limit intelligence agencies from using bulk acquisition warrants in a manner that exceeds what is strictly necessary to accomplish their objective because of U.K. intelligence agencies' past clandestine conduct.[189] Because intelligence agencies kept neither the public nor Parliament updated regarding their use of

181. *See* Davis v. Sec'y of State for the Home Dep't [2015] EWHC (Admin) 2092 [15]–[16].

182. *See Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 42.

183. *See supra* notes 86–89.

184. *See Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 51.

185. *See id.* ¶ 47.

186. *See* Investigatory Powers Act 2016, c. 25 (UK), § 158(1).

187. *See Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 33.

188. *See infra* Section III.C.

189. *See* Privacy Int'l v. Sec'y of State for Foreign and Commonwealth Affairs, Case No. IPT/15/110/CH, Judgment, ¶¶ 10–15, 84 (July 29, 2016), http://www.ipt-uk.com/docs/Bulk_Data_Judgment.pdf (discussing the collection of data that has been ongoing for seventeen years without oversight) [https://perma.cc/2VS4-FPHC].

bulk acquisition powers under Section 94 of the Telecommunications Act, practical experience and objective reality dictate that intelligence agencies should first meet substantive safeguards before accessing personal data.[190] To that point, *Digital Rights Ireland* and *Tele2 Sverige AB* both instruct that national legislation must provide "*clear and precise rules* indicating in what circumstances and under which conditions" a telecommunications provider is required to grant intelligence agencies access.[191] The IP Act's undefined operative phrases are far from clear and precise and could potentially be used as umbrella phrases to encompass whatever data an intelligence agency desires.

Next, the IP Act's provisions regarding the validity of operational purposes is insufficient to limit data access to solely what is necessary because the list of valid operational purposes is confidential and the secretary of state may approve any recommended operational purpose so long as it is more specific than "in the interests of national security" or "preventing or detecting serious crime."[192] The incentive to keep operational purposes secretive is blatant and fair—if an identified terrorist or criminal was aware that GCHQ was acquiring bulk data from Facebook, the user would obviously no longer communicate through Facebook.

However, that should not permit the standard of approval for an operational purpose to be set so low that merely adding the slightest degree of specificity suffices.[193] Otherwise, the procedural requirements become nugatory and do not restrict the issuance of bulk acquisition warrants to what is strictly necessary.[194] Though a U.K. document claims that operational purposes will contain "granular detail," the IP Act, as written, permits quite the opposite and creates a risk that the judicial commissioner and secretary of state will give too much deference to intelligence agencies.[195] Intelligence agencies may be in the best position to request relevant information, but after the Snowden revelations and the *Privacy International* judgment, it is paradoxical to give intelligence agen-

190. *See infra* Section III.C.

191. *Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 54; *Tele2 Sverige AB*, 2016 E.C.R. 970, ¶ 117 (emphasis added).

192. *See supra* notes 139–147.

193. *See id.*

194. *Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 54.

195. *See supra* note 146.

cies as much control as they currently have over operational purposes.[196]

Even though bulk acquisitions warrants are subject to obligatory review by a judicial commissioner—a key requirement of *Digital Rights Ireland*—this mere element alone does not ensure that bulk acquisition warrants are issued solely for what is necessary.[197] This is particularly evident because the reviewing judicial commissioner reviews the secretary of state's decision to issue a warrant based on the undefined criteria above.[198] Statutory interpretation does not provide grounds for a judicial commissioner to determine whether a warrant is necessary in the interests of national security or whether an operational purpose is valid.[199]

C. *Making the Investigatory Powers Act Compatible with the Charter of Fundamental Rights*

The statistics surrounding digital communications give merit to the United Kingdom's desire to legalize bulk acquisition surveillance powers.[200] In 2012, individuals around the world sent over thirty-five billion text messages or online messages through products ranging from standard desktops to innovative mobile devices.[201] On one hand, the vast capabilities are great for users, but on the other hand, intelligence agencies worry that technological advancements are making it harder to maintain strong intelligence on terrorists and criminals who increasingly communicate through these diverse channels.[202]

Because this fear is legitimate, this Note does not propose that bulk acquisition of data is categorically invalid. Rather, it introduces three modest proposals to ensure that bulk acquisitions warrants are granted and used only insofar as is necessary to (1) limit the scope of the investigatory powers vested through the phrase "in the interests of national security"; (2) add objective criteria before a secretary of state may validate an operational pur-

196. See Privacy Int'l v. Sec'y of State for Foreign and Commonwealth Affairs, Case No. IPT/15/110/CH, *supra* note 189; *see* Edward Malnick, *Home Secretary Theresa May Insists GCHQ Needs 'Haystack' of Data to Find 'Needle'*, Telegraph (Oct. 16, 2014), http://www.telegraph.co.uk/news/uknews/law-and-order/11167349/Home-Secretary-Theresa-May-insists-GCHQ-needs-haystack-of-data-to-find-needle.html [https://perma.cc/FAK4-KZ8M].

197. *Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 62.

198. *See id.*

199. *See id.*

200. *See* Operational Case for Bulk Powers, *supra* note 47, ¶¶ 3.4–3.6.

201. *See id.* ¶ 3.4.

202. *See id.* ¶¶ 3.5–3.6.

pose; and (3) create a new provision that alerts an individual whose data has been accessed at a time when that disclosure will not jeopardize the intelligence agencies' operation. The first criterion is subjective; the second criterion is objective; and the third criterion is a requirement taken directly from *Tele2 Sverige AB*.

1. Providing Limitations on the Phrase "In the Interests of National Security"

Defining, or at the very least limiting, the IP Act's operative phrase "in the interests of national security" is crucial to constraining the circumstances under which intelligence agencies may obtain a bulk acquisition warrant.[203] This Note proposes two criteria that the applying intelligence agency must produce to demonstrate why the warrant is necessary in the interests of national security. The purpose of these criteria is to ensure that the reviewing party's subjective determination on the warrant is *not* made on arbitrary grounds.

Though national security is an amorphous phrase—likely left undefined to account for unpredictable situations—the designation will be rendered meaningless unless it is given confines.[204] In the United States, commentators already caution that politicians' recent use of the phrase increasingly equates to "blatant opportunism"—a scheme to attach attenuated policies to the phrase because, in theory, there should be little resistance to such policies.[205] Few would contest that acquiring data to prevent a terrorist attack is in the interest of national security.[206] However, what about acquiring data to prevent an insurgent political candidate from winning an election against an incumbent?[207] Bright-line

---

203. This Note is not prepared to propose a workable definition of the phrase "national security" and acknowledges the difficulty in drawing bright-line rules in this area. Instead, it proposes a limitation.

204. *See* Laura K. Donohue, *The Limits of National Security*, 48 Am. Crim. L. Rev. 1573, 1579–82 (2011) (providing extensive background about the evolution of the phrase "national security").

205. *Id.* at 1753. Interestingly, this problem antedates recent developments as illustrated by the Supreme Court in *United States v. U.S. District Court*. *See* 407 U.S. 297, 314 (1972). Justice Powell wrote about the danger of abuse in framing issues in the matter of domestic and national security. *See id.* At one point, he quoted Michigan Senator Philip Hart about Hart's fear: "[T]his is my fear—we are saying that the President on his motion, could declare—name your favorite poison—draft dodgers, Black Muslims, the Ku Klux Klan, or civil rights activists to be a clear and present danger to the structure of the Government." *Id.*

206. *See id.* at 303.

207. *See* Lee Smith, *Did the Obama Administration's Abuse of Foreign-Intelligence Collection Start Before Trump?*, Tablet Mag. (Apr. 5, 2017), http://www.tabletmag.com/jewish-news-

rules are difficult to apply in the national security field and, under the IP Act's framework, the reviewing party will ultimately need to make a subjective determination.[208]

To assist with this subjective determination, a U.S. law, the Omnibus Crime Control and Safe Streets Act (Omnibus),[209] provides guidance on limiting the scope of the phrase "in the interests of national security."[210] Omnibus allows authorized applicants to obtain a warrant to intercept wire, oral, or electronic communications subject to prior judicial review.[211] Though Omnibus did not define the phrase "national security," it did require the applicant to provide specific written criteria to the reviewing judge.[212] The IP Act can limit data access under the guise of "national security" by requiring the intelligence agency to include criteria similar to that which is in Omnibus.[213]

First, the applying intelligence agency should, in a written affidavit, state its opinion and supporting rationale as to why the warrant is necessary in the interest of national security.[214] This should detail the intelligence agencies' evaluation on the potential risk to national security, the facts and circumstances that give rise to the warrant's necessity, and the investigative procedures that have already been used or could be used to alternatively accomplish the goal of the warrant.[215] Second, the applying agency should detail the intelligence agency's estimation regarding the impact that a failure to grant the warrant may have on national security interests. Because the IP Act's warrant review process is not adversarial,[216] it

---

and-politics/229062/did-the-obama-administrations-abuse-of-foreign-intelligence-collection-start-before-trump (suggesting that the Obama administration may have used surveillance abilities to monitor conversations of domestic political opponents) [https://perma.cc/5PKU-VWDM].

208. *See* Donohue, *supra* note 204, at 1579–82 (discussing the broad nature and lack of standards for "national security" justifications).

209. Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510–20 (1968).

210. The United States, like the United Kingdom, is guilty of the same omission in many of its own statutes. *See id.* (noting that neither the U.S. National Security Act, which refers to "national security" more than one-hundred times, nor the more recent Patriot Act, which uses the term over twenty-four times, define the term "national security").

211. *See id.* § 2516 (authorized applicants are generally attorney generals or assistant attorney generals).

212. *See id.* § 2518(1) (requiring that "[e]ach application for an order authorizing or approving the interception of . . . electronic communication . . . shall be made in writing upon oath or affirmation to a judge of competent jurisdiction . . . .").

213. *See, e.g.*, *id.* § 2518(4) (specifying requirements for "[e]ach order authorizing or approving the interception of . . . electronic communication . . . .").

214. *See id.* § 2518(1).

215. *See id.*

216. *See* Investigatory Powers Act 2016, c. 25 (UK), §§ 158–75.

is crucial that the intelligence agency be held accountable for its representations.

Several counterarguments must be addressed in turn. First, despite arguments to the contrary, the reviewing parties of bulk acquisition warrants are both competent and able to understand complex intelligence matters.[217] The secretary of state is qualified as an appointee of the prime minister and head of the U.K. department responsible for security and terrorism.[218] Likewise, a judicial commissioner is qualified due to the requirements that appointment only be made if the individual previously held a high judicial office and was jointly recommended by a combination of five political and judicial officials.[219] Like in the United States, where federal judges are capable of comprehending complex issues involving national security, the same is true of U.K. officials.[220]

Second, some may gripe with the encumbrance this imposes on intelligence agencies, especially in urgent times. However, this burden is necessary. As the U.S. Supreme Court stated in *United States v. U.S. District Court*, a case interpreting Omnibus, "[t]he circumstances described do not justify complete exemption . . . from prior judicial scrutiny . . . . Security surveillances are especially sensitive because of the inherent vagueness of the [national] security concept . . . and the *temptation to utilize such surveillances to oversee political dissent*."[221] To comply with the CFR, *Digital Rights Ireland*, and *Tele2 Sverige AB*, the IP Act must reduce citizens' uneasiness and apprehension that accompany GCHQ's and MI5's use of the unique power.[222] Moreover, in urgent situations, *Tele2 Sverige AB* permits an exception from the general rule of judicial or administrative review.[223] Additionally, if the circumstances necessitate omitting the proposed written affidavit requirement, it would be acceptable to substitute an emergency oral hearing in its place. In sum, compelling intelligence agencies to produce certain information to aid the secretary of state and judicial commissioner's subjective determination presumably will slow those reviewing parties

217. *See* United States v. U.S. Dist. Court, 407 U.S. 297, 320 (1972).

218. *See Ministerial Role: Secretary of State for the Home Department*, Gov.UK, https://www.gov.uk/government/ministers/secretary-of-state-for-the-home-department (last visited Sept. 10, 2017) [https://perma.cc/8VND-K4YG].

219. *See* Investigatory Powers Act 2016, c. 25 (UK), §§ 227(2), (4).

220. *See U.S. Dist. Court*, 407 U.S. at 320–21.

221. *Id.* at 320 (emphasis added).

222. The CFR, *supra* note 18, art. 7, 8, 52(1); *see Digital Rights Ireland*, 2014 E.C.R. I-238, ¶¶ 25–37; *Tele2 Sverige AB*, 2016 E.C.R. 970, ¶¶ 99–101.

223. *See Tele2 Sverige AB*, 2016 E.C.R. 970, ¶ 120 (establishing an exception to judicial or administrative review in "cases of validly established urgency").

from applying a rubber stamp to bulk acquisition warrants upon hearing the phrase "national security."

2. Incorporating Objective Criteria to Analyze Operational Purposes

Currently, under Section 161 of the IP Act, the secretary of state may only approve of an intelligence agency's operational purpose if that purpose is more specific than the broad phrases articulated in Section 158: in the interests of national security, preventing or detecting serious crime, or in the economic well-being of the United Kingdom so long as that interest is related to the U.K's national security interests.[224] Given this minimal threshold, the standard for a valid operational purpose should be amended to require an intelligence agency to answer to objective criteria before a secretary of state may validate an operational purpose.[225] At a minimum, these objective criteria should include the following: (1) identifiability; (2) quantity; and (3) purpose specification.[226]

The first criterion, identifiability, would require the intelligence agency to specify in the operational purpose whose data it seeks to acquire, the time frame it seeks to acquire the data for, and where that data is located. The purpose of this criterion is to ensure that the operational purpose is not merely boilerplate, but rather narrowly tailored to some degree. Though intelligence agencies may resist such a requirement as too tedious, there is reason to believe that this is not overly burdensome since metadata is already categorized and allows for cross-referencing.[227] Even if this requirement is slightly burdensome, intelligence agencies will need to maintain a list of individuals' data that have been accessed to notify those individuals at a time when it will no longer jeopardize the intelligence operation, as required by the CJEU in *Tele2 Sverige AB*.[228]

The second criterion, quantity, requires the intelligence agency to specify the aggregate amount of data it seeks to obtain. This is particularly important given the CJEU's concern in *Digital Rights Ireland* that the Data Retention Directive covered all users of the

224. *See* Investigatory Powers Act 2016, c. 25 (UK), § 158(1)–(2).

225. *See Tele2 Sverige AB*, 2016 E.C.R. 970, ¶¶ 110, 119.

226. *See* Erika McCallister et al., U.S. Dep't of Commerce: Nat'l Institute of Standards & Tech., Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) ES-2 (2010). The aforementioned criteria are inspired by a publication from the U.S. National Institute of Standards and Technology that expressed concern about the lack of protection of individuals' personally identifiable information.

227. *See* Moody, *supra* note 136.

228. *See Tele2 Sverige AB*, 2016 E.C.R. 970, ¶ 121.

Internet and thus practically interfered with the rights of the entire E.U. population.[229] By forcing the intelligence agency to represent in the operational purpose the quantity of data that it seeks to obtain, the secretary of state will have quantifiable statistics to guide their decision on whether the operational purpose is valid. Without such a requirement, intelligence agencies may seek to obtain data about virtually all U.K. citizens through an operational purpose that targets data retained by a behemoth telecommunications provider like Google.

The third criterion, purpose specification, requires the intelligence agency to specify not only which Section 158 umbrella phrase the warrant falls under, but also the granular detail for which the intelligence agency represents it will use the data.[230] Because operational purposes are covert, there is a need to ensure the public that the reviewing secretary of state and judicial commissioner are fully informed. Requiring an intelligence agency to provide specifics regarding its operational purpose to a secretary of state does not produce concerns that terrorists or criminals will find out and stop using specific services. That concern only exists if the operational purposes are disclosed to the public. Again, this language must not be boilerplate because intelligence agencies will otherwise have the incentive to go beyond what is strictly necessary for the stated operational purpose.

3. Notifying Individuals That An Intelligence Agency Accessed Their Data When Disclosure Will Not Jeopardize the Operation

Finally, the IP Act should be amended to require intelligence agencies to notify an individual whose data had been acquired at a point in time when such disclosure will not affect the intelligence operation. The CJEU articulated this requirement in *Digital Rights Ireland* and again in *Tele 2 Sverige AB*, the latter being a case decided shortly after the IP Act was enacted.[231] Without this notification, an individual will never know that his data had been accessed and thus will not be able to seek any legal remedy provided by Article 15(2) of the E-Privacy Directive and Article 22 of the Data Protection Directive.[232]

---

229. *Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 56.

230. *See* Operational Case for Bulk Powers, *supra* note 47, at 24.

231. *Tele2 Sverige AB*, 2016 E.C.R. 970.

232. *See supra* notes 52–53, 118.

D. *Brexit's Impact on the Future of Data Retention and Access Laws in the United Kingdom*

Notwithstanding these solutions, U.K. citizens voted in a June 2016 referendum (Brexit) to leave the European Union.[233] Though Brexit is a far cry from the numerous steps the United Kingdom must undertake to achieve complete independence, the United Kingdom's secession from the European Union would foreclose the CJEU's jurisdiction over the United Kingdom and remove the CFR's binding nature over the United Kingdom, absent an agreement stating otherwise.[234] On March 29, 2017, the United Kingdom commenced the secession process by exercising its Article 50 right and informing the European Council of its formal intent to abandon its European Union membership.[235] However, to gain complete independence from the European Union, the United Kingdom must still negotiate a withdrawal agreement with the European Council within two years of this initial withdrawal notice.[236] If no agreement is reached, then E.U. treaties will become inapplicable to the United Kingdom.[237]

This Note remains relevant even if the United Kingdom ultimately secedes from the European Union because the United Kingdom's future political and economic success will not be wholly detached from the success of the European Union.[238] Theresa May noted as much in her letter to the European Council, stating that the United Kingdom seeks a "deep and special partnership" with the European Union moving forward.[239] Pertinently, Prime Minister May acknowledged that security—the fight against crime and terrorism—is among her top priorities in the negotiations moving forward with the European Union.[240] Because the CJEU's recent judgments regarding data privacy under E.U. law lean heavily towards safeguarding individuals' privacy rights, it seems likely

233. Alex Hunt & Brian Wheeler, *Brexit: All You Need to Know About the UK Leaving the EU*, BBC NEWS (July 13, 2017), http://www.bbc.com/news/uk-politics-32810887 (the referendum is commonly referred to as "Brexit") [https://perma.cc/SGW8-768Q]. The United Kingdom utilized its Article 50 right of the Treaty of Lisbon to leave the European Union. *See* Treaty of Lisbon, *supra* note 60, art. 49A ("Any Member State may decide to withdraw from the Union in accordance with its own constitutional requirements.").

234. Hunt & Wheeler, *supra* note 233.

235. *See Theresa May's Letter Invoking Article 50*, N.Y. TIMES (Mar. 29, 2017), https://www.nytimes.com/2017/03/29/world/europe/theresa-may-letter-article-50.html?_r=0 [https://perma.cc/4VRJ-JVSL].

236. *See* Treaty of Lisbon, *supra* note 60, art. 49A.

237. *See id.*

238. *See Theresa May's Letter Invoking Article 50*, *supra* note 235.

239. *Id.*

240. *See id.*

that the CJEU's judgments interpreting Articles 7 and 8 of the CFR will be front and center in upcoming negotiations.[241]

Conclusion

Whether Edward Snowden's decision to reveal the surveillance policies of both the United States and the United Kingdom was honorable or treasonous will be an enduring debate for years to come.[242] Though there may be no consensus to that debate, the recent CJEU judgments, *Digital Rights Ireland* and *Tele2 Sverige AB*, unequivocally impose mandatory requirements on data access and data retention laws.[243] When read against these judgments, the IP Act unjustifiably interferes with the CFR due to its failure to limit or define the operative phrases that the secretary of state and reviewing judicial commissioner must consider when deciding whether to issue a bulk acquisition warrant. Bulk data access may very well be necessary for U.K. intelligence agencies to preserve national security and prevent serious crime.[244] However, these abilities must be balanced with the fundamental rights preserved in human rights jurisprudence. GCHQ's and MI5's past enigmatic uses of surveillance powers necessitate increased oversight and compliance with *clear and precise* conditions before a secretary of state may issue a bulk acquisition warrant. Albert Einstein once warned that "[n]o problem can be solved from the same level of consciousness that created it."[245] The IP Act, as written, contains the same overbreadth that the Telecommunications Act possessed. Seventeen years of concealing intelligence capabilities and clandestine operations was enough.[246] In a world that is becoming increasingly technologically dependent, precautions must be taken to balance the fundamental rights of privacy and data protection with efforts to maintain a high level of national security.

---

241. *See Digital Rights Ireland*, 2014 E.C.R. I-238; *Tele2 Sverige AB*, 2016 E.C.R. 970, ¶¶ 50, 125.

242. *See* Zach Schonfeld, *Most Americans Think Snowden Did the Right Thing, Poll Says*, Newsweek (June 2, 2014), http://www.newsweek.com/most-americans-think-snowden-did-right-thing-poll-says-253163 (providing survey results indicating that the American population is divided on whether Snowden did the right thing in exposing PRISM) [https://perma.cc/8N5G-P9WG].

243. *Digital Rights Ireland*, 2014 E.C.R. I-238, ¶ 54; *Tele2 Sverige AB*, 2016 E.C.R. 970, ¶¶ 110, 116–21.

244. *See supra* note 154.

245. Debbie Woodbury, *My No. 1 Tip for Solving Problems*, Huffington Post (May 2, 2013), http://www.huffingtonpost.com/debbie-woodbury/problem-solving-advice_b_3185536.html [https://perma.cc/6K89-S4BR].

246. *See* Travis, *supra* note 43.