Brooklyn Journal of International Law

Volume 43 | Issue 1 Article 30

12-12-2017

The Scrivener's Secrets Seen Through the Spyglass: GCHQ and the International Right to Journalistic Expression

Matthew B. Hurowitz

THE SCRIVENER'S SECRETS SEEN THROUGH THE SPYGLASS: THE GCHQ AND THE INTERNATIONAL RIGHT TO JOURNALISTIC EXPRESSION

INTRODUCTION

The Edward Snowden[1] leaks ("Snowden leaks") painted a clear picture of contemporary government surveillance and data storage. While government-sanctioned warrantless hoarding of personal data was once thought of as a problem exclusive to those intrusive, "freedom-hating" governments of the world, the Snowden leaks pulled back the curtain and painted a very different picture.[2] The Snowden leaks revealed that several nations, up until the date of the historic article published by *The Guardian* in the summer of 2013, that were perceived as relatively strong on issues of personal privacy, had engaged in the bulk collection of their citizen's communications data, or "metadata," as it is sometimes known.[3] The public discovered

---

1. Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013, 9:00 AM), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. *The Guardian* describes Snowden as:

> The individual responsible for one of the most significant leaks in US political history . . . a 29-year-old former technical assistant for the CIA and current employee of the defence contractor Booz Allen Hamilton. Snowden has been working at the National Security Agency for the last four years as an employee of various outside contractors, including Booz Allen and Dell.

Id.

2. Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 293 (2015).

3. Jemima Stratford, The *Snowden "Revelations": Is GCHQ Breaking the Law?* 2014 EUR. HUM. RTS. L. REV. 129, 132 (2014); Nicky Woolf, *How The Guardian Broke the Snowden Story*, ATLANTIC (July 5, 2013), http://www.theatlantic.com/national/archive/2013/07/how-i-the-guardian-i-broke-the-snowden-story/277486/; Greenwald et al., *supra* note 1. *The Guardian*, a British Newspaper first published in 1821, grew to achieve national and international recognition in the late nineteenth and early twentieth century. *See* Peter Osnos & Clive Priddle, *How Britain's Guardian Is Making Journalism History*, ATLANTIC (July 12, 2011), http://www.theatlantic.com/interna-

that the United States' National Security Agency (NSA) and the United Kingdom's Government Communications Headquarters (GCHQ) acquired bulk electronic data, which was collected through the interception of internet, email, and telephone use and shared that data between one another.[4] These electronic data collection schemes are subject to these nation's domestic laws, as well as the international agreements to which they accede. The United Kingdom is subject to the jurisdiction of the European Court of Human Rights (ECtHR), where issues that fall under the scope of the European Convention on Human Rights (ECHR) are resolved.[5]

The bulk acquisition of metadata is an issue that the ECtHR and other European courts[6] have explored through the scope of

---

tional/archive/2011/07/how-britains-guardian-is-making-journalism-history/241803/; *History of the Guardian*, GUARDIAN (June 5, 2002), https://www.theguardian.com/gnm-archive/2002/jun/06/1. While it started as a weekly paper covering news relevant to the greater Manchester area, it has now expanded to include extensive digital operations and covers worldwide issues, such as the Julian Assange leaks and the Rupert Murdoch phone and data hacking scandal. *Id.*

4. Stratford, *supra* note 3, at 129–30.

5. The ECtHR is a court that focuses exclusively on issues of human rights in the nations subject to its jurisdiction. *Profile of The European Court of Human Rights,* INT'L JUST. RESOURCE CENTER, http://www.ijrcenter.org/european-court-of-human-rights/ (last visited Jan. 16, 2017). The ECtHR began operating in 1959 and has delivered more than 10,000 judgments regarding alleged violations of the ECHR. *Id.* The ECtHR has jurisdiction to decide complaints submitted by individuals and States concerning violations of the ECHR, which principally concerns civil and political rights. *Id*. It cannot, however, take up a case on its own initiative. *Id.* Notably, the person, group or nongovernmental organization submitting the complaint does not have to be a citizen of a State Party. *Id.* Complaints submitted to the ECtHR, however, must concern violations of the ECHR allegedly committed by a State Party that directly and significantly affected the applicant. *Id.*

6. *See* EUR. CT. HUM. RTS., FACT SHEET—MASS SURVEILLANCE (2017), http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf [hereinafter Mass Surveillance Fact Sheet].

Articles 8[7] and 10[8] of the ECHR.[9] These Articles convey positive rights to privacy and expression for all persons who fall within the ECHR's jurisdiction.[10] As stated in a recent case before the Investigatory Powers Tribunal (IPT),[11] a tribunal created to ensure that the United Kingdom meets its international human rights obligations:

---

7. The exact language of Article 8 reads:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR Art. 8].

8. The exact language of Article 10 reads:

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Convention for the Protection of Human Rights and Fundamental Freedoms art. 10, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR Art. 10].

9. *See* Mass Surveillance Fact Sheet, *supra* note 6.

10. *See* ECHR Art. 8, *supra* note 7; ECHR Art. 10, *supra* note 8.

11. *See General Overview and Background*, INVESTIGATORY POWERS TRIBUNAL, http://www.ipt-uk.com/content.asp?id=10 (last visited Jan. 16, 2017). The IPT describes itself in its own words by stating that:

> Communications data, therefore, comprises, or includes, the date and time on which a call or electronic communication is made and received, the parties to it, the apparatus by which it is made and received and, in the case of a mobile telephone communication, the location from which it is made and in which it is received. It can include billing records and subscriber information. Just about the only information not included is the content of communications.[12]

When the ECtHR evaluates states' alleged violations of freedom of expression, it calculates into its holdings a counterbalancing of government interests—often interests of national security—with the maintenance of a democratic society.[13] What the ECtHR fails to properly take into account in its calculations, however, is the chilling effect that modern surveillance can have on journalists' ability to procure confidential sources and properly convey messages that are essential to the functioning of a democratic society.[14]

> The Tribunal was established to ensure that the United Kingdom meets its obligations under Article 13 of the European Convention on Human Rights (ECHR). . . . The Tribunal is an independent court. It decides complaints under the Regulation of Investigatory Powers Act 2000 (RIPA) and claims under the Human Rights Act 1998 (HRA). It considers allegations of unlawful intrusion by public bodies, including the Security and Intelligence Agencies (SIAs), the Police and local authorities . . . RIPA is the statute and main source of law that establishes and regulates the power of public bodies to intrude upon the privacy of members of the public. RIPA provides an avenue of complaint when these powers are believed to have been used unlawfully—the Tribunal.

Id.

12. Privacy International v. Secretary of State for Foreign & Commonwealth Affairs [2016] H.R.L.R. 21, [26].

13. *See, e.g.*, Liberty (The National Council of Civil Liberties) v. GCHQ & Others [2015] H.R.L.R. 2; Özgür Gündem v. Turkey, 31 Eur. H.R. Rep. 49 (2000); Valya Filipov, *Standards of Protection of Freedom of Expression and the Margin of Appreciation in the Jurisprudence of the European Court of Human* Rights, 17 COV. L.J. 64, 64–70 (2012).

14. *See* PEN AM. CENTER, GLOBAL CHILLING: THE IMPACT OF MASS SURVEILLANCE ON INTERNATIONAL WRITERS 5–6 (2015), http://www.pen-international.org/wp-content/uploads/2015/01/Global-Chilling_01-05-15_FINAL.pdf; Emily Bell et al., *Comment to Review Group on Intelligence and Communications Technologies Regarding the Effects of Mass Surveillance on*

This Note will explore the claim that the British government's acquisition of metadata stifles the activities of journalists, both inside and outside of its borders, in contravention of the freedom of journalistic expression contained within Article 10 of the ECHR.[15] This Note will show that said freedom of journalistic expression is a pillar of a democratic society that is not justifiably stifled by a countervailing national security interest. Part I of this Note will explore the historical and social background of the Snowden leaks, as well as the history of the GCHQ, detailing what the institution does at present, and the statutory framework under which it operates its acquisition of metadata.[16] This Part will also detail positive and negative reactions from public and private actors to both the data drop and the actions of the GCHQ. Part II will discuss the framework used by the ECtHR when evaluating alleged breaches of the right to freedom of expression, as well as precedent cases heard in front of both the ECtHR and the IPT, evaluating claims of Article 8 and 10 violations brought by individual citizens and international organizations due to electronic surveillance.[17] Part III will then address the national security interests that advocates of electronic surveillance put forth as justifications that metadata collection is necessary in a democratic society.[18] These advocates of electronic surveillance posit that surveillance's ability to prevent loss of human life and limb outweighs any privacy or freedom of expression interests.[19] This Part will then explore the chilling effect that electronic surveillance, particularly the collection of metadata, has on journalists' ability to procure anonymous

---

the Practice of Journalism, TOW CENTER FOR DIGITAL JOURNALISM 1–2 (Oct. 10, 2013), http://towcenter.org/wp-content/uploads/2013/10/Letter-Effect-of-mass-surveillance-on-journalism.pdf.

15. PEN AM. CENTER, *supra* note 14, at 5–6; Bell et al., *supra* note 14, at 1–2.

16. Stratford, *supra* note 3, at 129–41.

17. *See* EUR. CT. HUM. RTS., FREEDOM OF EXPRESSION IN EUROPE: CASE-LAW CONCERNING ARTICLE 10 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 7–10 (2007), http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-18(2007).pdf [hereinafter Freedom of Expression in Europe].

18. *Id.*

19. Richard A. Epstein, *The ECJ's Final Imbalance: It's Cavalier Treatment of National Security Issues Poses Serious Risk to Public Safety and Sound Commercial Practices*, 12 E.C.L. REV. 330, 332–33 (2016).

sources and express themselves in a way where they can function as one of the pillars of a democratic society.[20] Finally, Part IV will set forth a three-part solution that the British government can undertake in order to ensure that its agencies, including the GCHQ, comport their behavior to better protect the Article 10 journalistic freedom of expression. This solution proposes a new legislative approach to data-gathering, a new philosophical approach to privacy, and a new administrative approach to judicial oversight for data-gathering agencies like the GCHQ.

I. THE STATE OF MODERN BRITISH SURVEILLANCE

This Part will examine how the 2013 Snowden leaks affected public perception of government surveillance in both the United States and the United Kingdom. This Part will then provide a brief history of the GCHQ and explore its modern day activities, with a particular focus on its collection of metadata and incidences of its overreach, which have been chronicled in news articles.[21] Finally, this Part will provide a detailed discussion on the primary statutory authority by which the British Parliament outlined the government collection of metadata, the Regulation of Investigatory Powers Act of 2000, as well as section 94 of the Telecommunications Act of 1984 ("section 94"), another statute under the authority of which the GCHQ collected metadata.[22]

A. The Snowden Leaks

In 2013, Edward Snowden, a former contractor for the NSA, publicly unveiled claims that the NSA conducted an operation of mass electronic data collection, consisting of several million telephone records.[23] *The Guardian* published these claims and then

20. *See* PEN AM. CENTER, *supra* note 14; Bell et al., *supra* note 14.

21. Stratford, *supra* note 3, at 129–41.

22. *Regulation of Investigatory Powers Act 2000,* LEGISLATION.GOV.UK, http://www.legislation.gov.uk/ukpga/2000/23/contents (last visited Sept. 29, 2017); Telecommunications Act 1984, c. 12, § 94 (Eng.).

23. *See* Deeks, *supra* note 2. In 1952, President Harry Truman created the NSA out of the Armed Forces Security agency, in order "to provide an effective, unified organization and control of the communications intelligence activities of the United States conducted against foreign governments." *A Short History of the NSA*, JURIST.ORG (July 22, 2013), http://www.jurist.org/feature/2013/07/nsa-overview-2.php; Bell et al., *supra* note 14. In 1975, the U.S

continued to work with Snowden in a symbiotic relationship, where Snowden supplied the information and *The Guardian* supplied the podium for a mass revelation of the hidden activities of U.S. and U.K. government-run organizations.[24]

In response to these leaks, both private and public entities within the United States shifted their behavior, whether to vocally denounce or support the programs, or to better suit their actions to what seemed to be an impending clash of privacy and security based rights.[25] One example of the former was a lawsuit[26] filed by the American Civil Liberties Union (ACLU)[27]

Congress discovered that the NSA existed and collected data of both foreign and U.S entities. *Id.*

24. Deeks, *supra* note 2, at 291, 293; Mark Young, *National Insecurity: The Impacts of Illegal Disclosures of Classified Information*, 10 ISJLP 367, 367 (2014); Owen Bowcott, *GCHQ Spied on Amnesty International, Tribunal Tells Group in Email*, GUARDIAN (July 2, 2015), https://www.theguardian.com/uk-news/2015/jul/01/gchq-spied-amnesty-international-tribunal-email; Ewen MacAskill et al., *Mastering the Internet: How GCHQ Set Out to Spy on the World Wide Web*, GUARDIAN (June 21, 2013), https://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet.

25. *See* Young, *supra* note 24.

26. ACLU v. Clapper, 785 F.3d 787, 792 (2d Cir. 2014); *ACLU v. Clapper—Challenge to NSA Mass Call-Tracking Program,* ACLU, https://www.aclu.org/cases/aclu-v-clapper-challenge-nsa-mass-call-tracking-program (last visited Jan. 16, 2016).

27. *ACLU History,* ACLU, https://www.aclu.org/about/aclu-history (last visited Jan. 16, 2016). The ACLU is a nonprofit, nonpartisan, and nongovernmental organization whose mission statement is to continue "to fight government abuse and to vigorously defend individual freedoms including speech and religion, a woman's right to choose, the right to due process, citizens' rights to privacy and much more." *Id.* The ACLU has historically advocated in what they viewed as the expansive power of the First Amendment when it comes to freedom of speech and freedom of expression in the United States. *Id.* One example of this is *Reno v. ACLU*, where the Supreme Court ruled in favor of the ACLU, holding that government blanket prohibitions on the transfer of obscene materials are unconstitutional content-based violations of free speech. Reno v. ACLU, 521 U.S. 844, 885 (1997).

against Director of National Intelligence,[28] James Clapper,[29] alleging that the NSA's call-tracking program violated the Fourth Amendment developed right to privacy[30] and the First Amendment encoded right to freedom of speech.[31] The Second Circuit found in favor of the ACLU's claim that the USA PATRIOT Act

---

28. After the attacks on U.S. domestic soil on September 11, 2001, the executive branch, under the leadership of President George W. Bush, moved towards strengthening its own intelligence capabilities, culminating in the creation of the Director of National Intelligence position. *History*, OFF. OF THE DIRECTOR OF NAT'L INTELLIGENCE, https://www.dni.gov/index.php/who-we-are/history (last visited Oct. 17, 2017). In parallel to the GCHQ, much of the strengthening of intelligence capabilities was at first done without direct legislative authority. *Id.* In April 2005, John D. Negroponte was appointed to be the first Director of National Intelligence. *Id.*

29. In August 2010, during the presidency of Barack Obama, James Clapper became the Director of National Intelligence. *Biography of James R. Clapper*, LINDSAY GRAHAM, UNITED STATES SENATOR SOUTH CAROLINA, PUBLIC DOCUMENTS, https://www.lgraham.senate.gov/public/_cache/files/d7b50e0c-6f70-417d-a8b6-5ab1000bb38a/the-honorable-james-r.-clapper-bio.pdf. (last visited Oct. 17, 2017). Prior to his service as Director, he worked in a multitude of active field positions within the Armed forces, in intelligence related positions within the U.S. Air Force, and as a consultant and advisor for myriad private and government agencies. *Id.* Director Clapper is noteworthy for his testimony before the U.S. Congress in March 2013, where he responded to an inquiry from Senator Ron Wyden of Oregon, who asked if the NSA, "collect(s) any type of data at all on millions or hundreds of millions of Americans?" Glenn Kessler, *Clapper's 'Least Untruthful' Statement to the Senate*, WASH. POST (June 12, 2013), https://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html?utm_term=.f96509d87eb4; Abby D. Phillip, *James Clapper Apologizes to Congress for 'Clearly Erroneous' Testimony*, ABC NEWS (July 2, 2013), http://abcnews.go.com/blogs/politics/2013/07/james-clapper-apologizes-to-congress-for-clearly-erroneous-testimony/. Clapper replied that the agency definitely does not do so wittingly. *Id.* This statement later brought outrage from the inquiring senator, the media, and the public, as it seemingly flew directly in the face of the Snowden leaks brought to light in June of the same year. *Id.*

30. U.S. CONST. amend. IV. Although the word "privacy" never appears in the text of the Fourth Amendment, whether the right to be secure in one's papers and effects extends to one's phone communications is, at the very least, a contested issue under U.S. Supreme Court common law. *See, e.g.*, Monu Bedi, *The Curious Case of Cell Phone Location Data: Fourth Amendment Mash-Up*, 110 NW. U. L. REV. 507, 507–10 (2016); David H. Hines, *Fourth Amendment Limitations on Eavesdropping and Wire-Tapping*, 16 CLEV.-MARSHALL L. REV. 467, 467 (1967).

31. U.S. CONST. amend. I.; *see also* MacAskill, *supra* note 24.

did not provide for the legality of a bulk telephone metadata collection program, remanding the case to a lower court in order to answer the questions of constitutionality.[32] Other examples of public outcry in connection with the Snowden leaks include protests across the United States, with one massive rally occurring at the nation's capital of Washington D.C.[33]

One example of an institutional shift in response to this data leak was when President Barack Obama ordered James Clapper to declassify information regarding a portion of the nature and methodology of the NSA's bulk data collection under section 501 of the Foreign Intelligence Surveillance Act.[34] In his accompanying statement to these disclosures, Clapper set forth an argument for the NSA's program by invoking the agency's administrative safeguards and an overriding national security interest.[35]

B. The History of the GCHQ and its Metadata Collection

The core justification for the GCHQ's work, which has been called "signals intelligence" or "Sigint," first came to rise in the form of Britain's Secret Security Bureau in 1909.[36] The overriding security interest of the time was a fear of German spies, retroactively justified by the first World War, which lasted from

---

32. *See Clapper*, 785 F.3d, at 821. According to a report prepared for Congress, "Congress passed the USA PATRIOT Act (the Act) in response to the terrorists' attacks of September 11, 2001. The Act gives federal officials greater authority to track and intercept communications, both for law enforcement and foreign intelligence gathering purposes." CONGRESSIONAL RES. CENTER, CRS REPORT FOR CONGRESS 1 (Apr. 18, 2002), https://fas.org/irp/crs/RS21203.pdf.

33. Protestors across the United States and within Washington D.C. itself gathered soon after the Snowden leaks, endorsing the Fourth Amendment right of privacy and condemning the NSA's electronic surveillance programs. Jim Newell, *Thousands Gather in Washington for Anti-NSA 'Stop Watching Us" Rally*, GUARDIAN (Oct. 26, 2013), https://www.theguardian.com/world/2013/oct/26/nsa-rally-stop-watching-washington-snowden; Rebecca Bowe, *NSA Surveillance: Protestors Stage Restore the Fourth Rallies Across US*, GUARDIAN (July 5, 2013), https://www.theguardian.com/world/2013/jul/04/restore-the-fourth-protesters-nsa-surveillance.

34. Young, *supra* note 24, at 375; Declassified, *DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA)*, IC on the Record—Office of the Director of National Security (Sept. 10, 2013), https://icontherecord.tumblr.com/post/60867560465/dni-clapper-declassifies-intelligence-community.

35. Young, *supra* note 24, at 376.

36. MacAskill et al., *supra* note 24.

1914 to 1918, and refined by the second World War, which lasted from 1939 to 1945.[37] The priorities of the GCHQ came into greater focus during the Cold War, which is commonly understood as the period between the end of the second World War and the fall of the Berlin Wall in 1991.[38] Attention on Moscow was easily justified, given the Cold War's heavy focus away from direct engagement and towards conflicts between proxies and battles fought by spies over covert intelligence.[39] During this time, and throughout the GCHQ's move to its present home in Cheltenham, the agency was acting under no statutory authority granted from Parliament.[40] Finally, in 1994, the Intelligence Services Act gave the GCHQ a leash from the legislature, albeit one that kept the agency's powers and objective obscure and ill-defined in its legalese.[41]

---

37. *Id.*

38. *Id.*; *Cold War*, BRITANNICA, https://www.britannica.com/event/Cold-War (last visited Sept. 19, 2017).

39. David Barrett, *Secret Files Reveal Techniques of Cold War Soviet Spies*, TELEGRAPH (Aug. 21, 2015), http://www.telegraph.co.uk/news/uknews/defence/11814627/Secret-files-reveal-techniques-of-Cold-War-Soviet-spies.html; Lauren Turner, *Cambridge Spies: Defection of 'Drunken' Agents Shook US Confidence*, BBC NEWS (Oct. 23, 2015), http://www.bbc.com/news/uk-34596824.

40. The reasoning behind how the GCHQ came to reside in a compound in Cheltenham, a town in the province of Gloucestershire, England, is long and somewhat contested. Bob Dormon, *INSIDE GCHQ: Welcome to Cheltenham's Cottage Industry*, REGISTER (May 24, 2013, 7:05 AM), http://www.theregister.co.uk/2013/05/24/geeks_guide_gchq/. What is certain is that Americans controlled bases at the two Cheltenham sites during World War II, which were operated as a communications hub for the European Theatre of Operations. *Id.* A staffer from the GCHQ visited the site after the war and promoted it to the agency in a favorable light. MacAskill et al., *supra* note 24. The GCHQ then moved to the area sometime in the early 1950s. *Id.* The present incarnation of the compound at Cheltenham is popularly referred to as "the doughnut," for the shape of its main building. *Id.* The area was redone in 2013 and contains two principle sites with over fifty buildings, many structured to resemble the buildings of Bletchley park, the historic home to the World War II Enigma codebreakers. *Id.*

41. The Intelligence Services Act statutorily defines the GCHQ by stating that:

> There shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be (b) to provide advice and assistance about—(i) languages, including terminology used for technical matters, and (ii) cryptog-

The Snowden leaks also implicated the GCHQ in the mutual exchange of metadata.[42] The leaked documents revealed a cross-Atlantic exchange of information in the form of telephone call records, as well as several significant aspects of citizens' online private lives.[43] A 2009 memo, which was sent between the director in charge of GCHQ's Mastering the Internet program and a senior member of the agency's cyber defense team, was summarized to the public in a 2013 article in *The Guardian*, explaining how the GCHQ collects more metadata than the NSA.[44] Further, the article highlighted the close relationship between the GCHQ and the NSA, created by the need for transatlantic cooperation in order to process the substantial volume of metadata.[45]

The United Kingdom has experienced similar displays of public outcry against the collection of metadata.[46] There are examples of political and surveillance experts who refer to proposed

---

> raphy and other matters relating to the protection of information and other material, to the armed forces of the Crown, to Her Majesty's Government in the United Kingdom or to a Northern Ireland Department or to any other organisation which is determined for the purposes of this section in such manner as may be specified by the Prime Minister.

Intelligence Services Act 1994 § 3, http://www.legislation.gov.uk/ukpga/1994/13/section/3 (Eng.); MacAskill et al., *supra* note 24.

42. Stratford, *supra* note 3, at 132.

43. *Id*.

44. The Mastering the Internet program, one of the two principal components of the GCHQ, involves, amongst other things, the interception of data leaving and entering the United Kingdom through fiber optics cables owned by private companies. Ewen MacAskill et al., *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications*, GUARDIAN (June 21, 2013, 12:23 PM), https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa; Kadhim Shubber, *A Simple Guide to GCHQ's Internet Surveillance Programme Tempora*, WIRED (June 24, 2014), http://www.wired.co.uk/article/gchq-tempora-101; MacAskill et al., *supra* note 24.

45. MacAskill et al., *supra* note 24.

46. *Regulation of Investigatory Powers Act 2000*, GUARDIAN (Jan. 19, 2009, 8:24 AM), https://www.theguardian.com/commentisfree/libertycentral/2009/jan/14/regulation-investigatory-powers-act; *The RIP Act*, GUARDIAN (Oct. 24, 2000, 12:25 PM), https://www.theguardian.com/world/2000/oct/24/qanda.

expansions of the present surveillance program as "totalitarian."[47] Moreover, there are public media reports of the GCHQ's overreach in its sweeping capture of emails from the foremost journalists in the western world, including twenty high-profile individuals, and human rights groups, such as Amnesty International.[48]

C. The GCHQ's Statutory Limitations Under the Regulation of Investigatory Powers Act 2000

British Parliament passed the Regulation of Investigatory Powers Act 2000[49] (RIPA) in order to, as they stated, allow law agencies access to current technologies for the purpose of fighting terrorists and other harmful nonstate agents.[50] RIPA

---

47. Matt Burgess, *UK Mass Surveillance "Totalitarian' and Will 'Cost Lives', Warns Ex-NSA Tech Boss*, WIRED (Jan. 6, 2016), http://www.wired.co.uk/article/mass-surveillance-william-binney-nsa-uk-ip-bill.

48. Amnesty International describes themselves as a:

> World-embracing movement working for the protection of human rights. It is independent of all governments and is neutral in its relation to political groups, ideologies and religious dividing lines. The movement works for the release of women and men who have been arrested for their convictions, the colour of their skin, their ethnic origin or their faith—provided that they have not themselves used force or exhorted others to resort to violence.

Amnesty International—History, NOBELPRIZE.ORG http://www.nobelprize.org/nobel_prizes/peace/laureates/1977/amnesty-history.html (last visited Jan. 16, 2017). *See also* Matthew Weaver, *Security Services Spied on 20 High-Profile People in Questionable Operations*, GUARDIAN (July 27, 2016, 9:41 AM) https://www.theguardian.com/world/2016/jul/27/mi5-and-gchq-spied-on-20-high-profile-people-in-questionable-*operations*; Burgess, *supra* note 47; James Ball, *GCHQ Captured Emails of Journalists from Top International Media*, GUARDIAN (Jan. 19, 2015, 10:04 AM), https://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post; Bowcott, *supra* note 24.

49. The year the bill was passed is notable. As stated in a Guardian article at the time, "[t]he government was keen to push the bill through parliament before the Human Rights Act became law in October 2000 in order to ensure that law agencies had a framework for covert surveillance that was compliant with the European convention on human rights." *Regulation of Investigatory Powers Act 2000*, *supra* note 46.

50. RIPA describes itself and its own purpose in its introductory text. Its self-stated goal is:

was passed as a direct response to the adversity with which the U.K.'s law stood against the ECtHR, as evidenced by cases like *Malone v. United Kingdom*.[51] In *Malone*, the petitioner claimed that it was unlawful for the British government to intercept his communications without his consent.[52] The United Kingdom, in turn, responded that there was no law that prevented them from doing so when they had procured a warrant for the purposes of tapping petitioner's phone.[53] The ECtHR found in favor of the petitioner, reasoning that Malone's ECHR Article 8 privacy rights had been violated.[54] The concurrence highlighted the ECtHR's interest in presiding over a case where the British government was attempting to become a master over the citizen's private life.[55] RIPA passed amidst much controversy, with several critics claiming that the provisions within the bill did not create

---

> To make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; to provide for commissioners and a tribunal with functions and jurisdiction in relation to those matters, to entries on and interferences with property or with wireless telegraphy and to the carrying out of their functions by the security service, the Secret Intelligence Service and the Government Communications Headquarters.

Regulation of Investigatory Powers Act 2000, Introductory Text, http://www.legislation.gov.uk/ukpga/2000/23/introduction (Eng.); *See Regulation of Investigatory Powers Act 2000*, *supra* note 46.

51. Malone v. the United Kingdom, 7 Eur. Ct. H.R. 14 (1985), http://hudoc.echr.coe.int/eng?i=001-57533; Laura K. Donohue*, Criminal Law: Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1164–66 (2006).

52. Malone v. the United Kingdom, *supra* note 51; Donohue*, supra* note 51, at 1064.

53. Malone v. the United Kingdom, *supra* note 51, at [61]; Donohue, *supra* note 51, at 1064.

54. Malone v. the United Kingdom, *supra* note 51, at [80]; Donohue, *supra* note 51, at 1065.

55. Malone v. the United Kingdom, *supra* note 51; Donohue, *supra* note 51, at 1065.

sufficient safeguards against abuse and that this system would result in a series of civil rights violations.[56]

RIPA distinguishes the interception of the contents of a communication, called content data, from the acquisition of information that is extrinsic to the actual contents of a communication, called communications data.[57] The Secretary of State must issue a warrant in order for an intelligence agency, like the GCHQ, to legally intercept content data.[58] Acquisition of communications data, on the other hand, is the process by which an applicant receives an authorization from a public authority to collect traffic data, service use information, or subscriber information, either from the relevant communications service provider or through their own interception of traffic.[59]

Communications data, also referred to in the public discourse as "metadata," is comprised of all of these data types and can compose the near-entirety of an individual's online, phone, and postal communications, with the exception of the actual content of those messages.[60] Traffic data is the information attached to a communication for the purposes of identifying it within transit.[61] This can include information identifying senders and recipients of communications, information regarding the physical location of a device that has sent out a communication, and surface web-browsing information such as a domain name of a visited website.[62] Service use information is data that conveys the use made of any communications service by any person.[63]

---

56. *Regulation of Investigatory Powers Act 2000*, *supra* note 46.

57. Stratford, *supra* note 3, at 132.

58. Regulation of Investigatory Powers Act 2000, c. 1, § 1–5, http://www.legislation.gov.uk/ukpga/2000/23/part/I/chapter/I/crossheading/unlawful-and-authorised-interception (Eng.).

59. Regulation of Investigatory Powers Act 2000, c. 2, § 21. Any operator who provides a postal or telecommunications service shall be considered a communications service provider in the framework of the statute whether they store their data, process their data, or provide a service completely inside or partially outside the U.K. Regulation of Investigatory Powers Act 2000, c. 1, § 2.

60. Stratford, *supra* note 3, at 132.

61. HOME OFF., ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA 15–18 (Mar. 2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf; Stratford, *supra* note 3, at 132.

62. HOME OFF., *supra* note 61, at 15–18.

63. Regulation of Investigatory Powers Act 2000, c. 2, § 21.

Service use information includes data regarding telephone numbers an individual has called, timing and duration of internet service he or she has used, and records of postal items he or she has sent.[64] Subscriber information is data that is held by communications service providers about the person to which they provide a service.[65] Subscriber information includes a communication service's account holder's billing information with the accompanying details and information regarding the identities of subscribers in connection with their email address, phone number, or other information provided to the service.[66]

The distinction between the interception of content data and the acquisition of communications data, as detailed within RIPA, is critical towards an analysis of its compliance with international human rights.[67] A government agent can procure communications data much easier than they can content data.[68] The authorization required to procure communications data is still to be issued by the government agent with proportionality in mind.[69] The safeguards around this authorization, however, amount to less of a safeguard than a warrant requirement.[70] Police officials and GCHQ officials do not need to go through a judge or the Secretary of State's office to obtain authorizations, but instead must request one from a designated member of their own organization.[71]

RIPA was created, in part, to address the disparity between the British government's surveillance schematic and the standards that the ECHR demands, as evidenced in *Malone*.[72] Accordingly, the legislation creates several legal safeguards, such as

64. *Id.*; HOME OFF., *supra* note 61, at 19.

65. Regulation of Investigatory Powers Act 2000, c. 2 § 21; HOME OFF., *supra* note 61, at 20.

66. HOME OFF., *supra* note 61, at 14.

67. Stratford, *supra* note 3, 132.

68. *Id.*

69. Regulation of Investigatory Powers Act 2000, c. 2, § 21.

70. Stratford, *supra* note 3, 132.

71. Regulation of Investigatory Powers Act 2000, c. 2, § 21; Ball, *supra* note 48.

72. Malone v. the United Kingdom, *supra* note 51, at [61]; Donohue, *supra* note 51, at 1059, 1064.

judicial and oversight functions, including the IPT as an available recourse for legal complainants.[73] These oversight safeguards, however, have received criticism, as the IPT has seldom ruled in favor of a claimant bringing suit against the government agencies conducting surveillance.[74]

RIPA's provisions on communications data do not make any special procedural exception for privileged or confidential information held or exchanged by business professionals or journalists.[75] Parliament's Acquisition and Disclosure of Communications Data Code of Practice ("Code of Practice"),[76] published in 2015, however, partially addresses this problem of vulnerable confidential information.[77] Applicants for authorizations for metadata that they know to belong to journalists, or other holders of confidential information, must claim as much on their application.[78] The Code of Practice then mandates that the public interests of the free press must be accounted for in a proportionality test, against the overriding government interest at hand.[79] Those applicants who are seeking communications data specifically for the purpose of identifying a journalist's sources must undergo a more thorough procedure, where they apply to a court for a production order.[80] This judicial approval, however, comes after the agency's own evaluation that the data sought falls within the bounds of what is exceedingly likely to determine a journalistic source.[81]

D. The GCHQ's Collection of Communications Data Under Section 94 of the Telecommunications Act of 1984

The GCHQ, as well as MI5, also collect and hold communications data outside of the legal framework of RIPA by relying on

---

73. *General Overview and Background*, INVESTIGATORY POWERS TRIBUNAL, http://www.ipt-uk.com/content.asp?id=10 (last visited Jan. 16, 2017).

74. Donohue, *supra* note 51, at 1171.

75. HOME OFF., *supra* note 61, at 45–48.

76. This disclosure issues non-binding instructions from Parliament to the U.K.'s executive agencies on how they are supposed to implement the data-gathering and retention statutes. *Id.* at 5.

77. *Id.*

78. *Id.*

79. *Id.*

80. *Id.*

81. *Id.* at 47.

section 94.[82] Section 94 allows the Secretary of State to give directions to individuals, including providers of electronic communications networks, as long as those directions appear to the Secretary, "to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom."[83] At the time of its enactment in 1984, section 94 allowed the Secretary of State to work with the telecom industries in a world where there were few networked computers and a smaller potential for sweeping data collection.[84] Since then, intelligence agencies, including the GCHQ, have used section 94 to procure directions from Secretaries of State in order to acquire bulk communications data from both foreign and domestic electronic service providers.[85] The GCHQ characterizes its bulk communications data in line with the definition of communications data within the RIPA framework. This data, however, is treated as though it were obtained pursuant to the RIPA provisions regarding the interception of content data.[86]

---

82. *Privacy International* [2016] 21 H.R.L.R., [19]; *see* Amberhawk Training, *Here's the Little-Known Legal Loophole that Permitted Mass Surveillance in the UK*, REGISTER (Nov. 9, 2015) http://www.theregister.co.uk/2015/11/09/hawktalk_wip/.

83. Telecommunications Act 1984, § 94(1), § 94(8), http://www.legislation.gov.uk/ukpga/1984/12/section/94 (Eng.).

84. *See* Amberhawk Training, *supra* note 82.

85. In response to a lawsuit against them claiming, amongst other things, that the GCHQ's collection of bulk communications data under section 94 was unlawful, the GCHQ provided the IPT with an account of their relevant operations, stating that:

> [In 1998 and then regularly] since 2001, GCHQ has sought and obtained from successive Foreign Secretaries a number of § 94 directions relating to the ongoing provision of various forms of bulk communications data. In keeping with GCHQ's external intelligence mission, the datasets received under these directions are predominantly foreign-focused, and the data acquired is accordingly in most cases only a fraction of that possessed by the [PECN's].

Privacy International [2016] H.R.L.R. 21, [10].

86. *Id.*

II. THE LEGAL FRAMEWORK BEHIND ECHR CLAIMS AGAINST ELECTRONIC SURVEILLANCE VIOLATIONS OF ARTICLE 10

The ECHR can, and should, be the mechanism by which courts analyze electronic surveillance schemes like those created by RIPA and section 94. This Part will demonstrate, piecemeal, how the ECHR treats freedom of expression when it is, arguably, threated by an electronic surveillance program. Through the course of the ECHR's jurisprudence regarding mass surveillance, courts have chosen to balance the rights inherent in Article 10, including freedom of journalistic expression, against countervailing government interests.[87] This Part will evaluate the legal framework used in finding governments' violations of Article 10's guarantee of freedom of expression. Then, this Part will highlight several cases that demonstrate the criteria under which the ECtHR and IPT evaluate claims that a government surveillance program violates either Article 8's right of privacy or Article 10's right to freedom of expression.[88] Taken together, this will demonstrate both the weighing of interests inherent in an Article 10 analysis, and the connection between privacy and expression that exists where electronic surveillance claims arise.

A. The Legal Framework of Article 10 Claims Alleging Violations of Freedom of Expression

There are three criteria that European courts have applied to measure whether a government interference with an individual's freedom of expression breaches Article 10.[89] The law or action that restricts expression must be done in pursuit of a legitimate government interest, it must be prescribed by law, and the restriction must be necessary in a democratic society.[90]

The ECtHR has determined what suffices as a legitimate government interest through case law.[91] Governments often argue national security as a justification for their surveillance activities, which the ECtHR usually accepts as a valid government interest.[92] It is not sufficient, however, that there be a legitimate

87. Freedom of Expression in Europe, *supra* note 17, at 7.
88. ECHR Art. 8, *supra* note 7; ECHR Art. 10, *supra* note 8.
89. Freedom of Expression in Europe, *supra* note 17, at 7–10.
90. *Id.*
91. *See id.*
92. *Id.* at 7.

government interest in order to supersede a breach of an individual's freedom of expression.[93] The government action must either be prescribed by law or supported by some legal basis for any restriction of expression.[94] This legal basis first must be found within domestic law, to which the government must obey.[95] The law in question must also contain a measure of accessibility and foreseeability, so that individuals may ensure that they are not deprived of their freedom of expression unfairly.[96]

The final criteria is that any restriction on freedom of expression must be necessary in a democratic society.[97] The strength of the government interest is weighed against the suppression of freedom of expression in order to determine whether the government is meeting a pressing social need.[98] The value of national security interests, mentioned in Article 10, has often been cited as supplying governments with a claim that an infringement on freedom of expression is necessary in a democratic society.[99] While states are given leeway, under the "margin of appreciation," to determine what qualifies as a necessity in a democratic society, it is ultimately up to the ECtHR to evaluate the strength of the interests at hand.[100] It is through this three-part test—legitimate government interest, prescribed by law, and necessary in a democratic society—that the court ruled in favor of the freedom of the Austrian press to defame politicians without fine imposition, [101] the freedom of a German citizen to defame judges for their ruling in a sensitive political case without conviction,

93. *Id.* at 8.

94. *Id.* (citing *Herczegfalvy v. Austria, judgment of 24 September 1992, Series A No. 244*).

95. Telegraaf Media Nederland Landelijke Media B.V. v. The Netherlands, 34 B.H.R.C. 193 at [90] (2012), http://hudoc.echr.coe.int/eng?i=001-114439.

96. *Id.*

97. Freedom of Expression in Europe, *supra* note 17, at 9.

98. *Id.*

99. *Id.*

100. As stated in a report on the ECHR, "[t]he member states have some discretion ('margin of appreciation') in assessing the existence of such a need. That margin is subject to European review, however, the extent of which will vary according to the case." *Id.*

101. *See* Lingens v. Austria, Application no. 9815/82, (1986) 8 Eur. H.R. Rep. 407, http://hudoc.echr.coe.int/eng?i=001-57523.

[102] and the freedom of several British newspapers to publish or disclose extracts from the memoirs of a former member of the British Security Services. [103]

B. The Legal Framework Behind ECHR Claims Against Electronic Surveillance

Even before *Malone*, the ECtHR recognized the need for both an element of transparency and an imminent state security interest in order to find a surveillance system in compliance with law and Article 8.[104] In *Klass v. Federal Republic of Germany*, in the context of a communications interception scheme, the court found German law was not in violation of Article 8 where authorities were required to notify citizens of the interception after the fact and, where there is an imminent danger to state security, other methods of obtaining the information are unavailable, and the surveillance ceases as soon as the other conditions are no longer met.[105]

Another case, *Weber & Saravia v. Germany*, represented a landmark decision in ECtHR surveillance jurisprudence with regards to both ECHR Articles 8 and 10.[106] The ECtHR found that

---

102. *See* Barthold v. the Federal Republic of Germany, Application No. 8734/79, (1985) 7 Eur. H.R. Rep. 383, http://hudoc.echr.coe.int/eng?i=001-57432.

103. The 1987 book, *Spycatcher,* written by Peter Wright, a retired member of British Security Services, experienced widespread publication and commercial success in the United States, while British newspapers, including *The Observer* and *The Guardian*, were barred from publishing excerpts of the novel. *See* Edwin McDowell, *'Spycatcher,' Banned at Home, Thrives in U.S.*, N.Y. TIMES (Aug. 1, 1987), http://www.nytimes.com/1987/08/01/books/spycatcher-banned-at-home-thrives-in-us.html. The British Security Services had, embedded in their practices, a culture of secrecy, which Britain's highest court effectuated when they initially held that British papers could not print excerpts of *Spycatcher*, following the U.K.'s argument that Peter Wright violated the Official Secrets Act, and his obligation of confidentiality, when he wrote the book. *See* The Observer and The Guardian v. United Kingdom, (1992) 14 Eur. H.R. Rep. 153 (holding that an injunction against the newspapers to prevent their publication of *Spycatcher* excerpts was in breach of Article 10, reasoning that the full publication of the novel in the United States made the government aim unnecessary and nonlegitimate).

104. Donohue, *supra* note 51, at 1059.

105. *Id.* (citing *Klass v. Federal Republic of Germany*, 2 Eur. H.R. Rep. 214 (1980)).

106. 46 SE5 Eur. H.R. Rep. 47 (2008).

protection against international terrorism was a sufficient justification to find no breach of petitioners' Article 8 and 10 rights, where the German government intercepted the contents of their communications.[107] The interception program became effective in order to identify issues of national security based on the interception of telecommunications containing specific keywords regarding hot button issues.[108] The ECtHR recognized the margin of appreciation that governments are given in the service of defining a national security interest as necessary in a democratic society.[109] The Court also took note of safeguards against abuse that could strengthen a government's case, where they had not acted in violation of this criteria.[110] The German program was found to be sufficiently foreseeable and to have adequate safeguards to qualify as appropriate under these standards with regards to general interception of communications.[111] One petitioner, a high-profile journalist, also argued that a breach of her Article 10 right had occurred due to the government collection of information regarding her confidential sources.[112] The ECtHR found that, where targeted interception of a journalist's data was not specifically for the purpose of discovering his or her confidential sources, safeguards that satisfy the requirements of Articles 8 and 10 suffice to maintain the integrity of these sources.[113]

In contrast with *Weber*, the ECtHR, in *Telegraaf Media Nederland Landelijke Media BV & Others v. Netherlands*, found that the Netherland's secret service violated ECHR Articles 8 and 10 where they intercepted communications of a newspaper in order to circumvent the protection of a journalistic source.[114] The ECtHR stated that the fact that government authorities had specifically targeted their surveillance on journalists for the express purpose of discovering a confidential source gave rise to a need for advanced safeguards or more proof of an overriding public

107. *Id.* at 61–69, 72–76.
108. *Id.* at 51–54.
109. *Id.* at 66.
110. *Id.* at 63.
111. *Id.* at 61–69.
112. *Id.* at 74.
113. *Id.* at 74–76.
114. 34 B.H.R.C. 193 at [80] (2012), http://hudoc.echr.coe.int/eng?i=001-114439.

interest.[115] While this is a recent case of the ECtHR upholding Article 10 interests against surveillance operations, the measures taken here were targeted towards content data, thus distinguishable from *Weber & Saravia*.[116]

In *Liberty (The Nat'l Council of Civil Liberties) v. GCHQ*, the IPT, in its evaluation of the communications interceptions system under RIPA, attached the *Weber* criteria to the protection of metadata.[117] The tribunal found, however, less of a strict adherence to safeguards necessary where the data acquired was merely the communications data used to identify those individuals whose content data had been intercepted.[118]

In *Privacy Int'l v. Sec'y of State for Foreign Affairs & Ors*, the IPT found that the GCHQ could, in accordance with ECHR Article 8, utilize the section 94 Secretary of State directions in order to lawfully collect bulk communications data outside of RIPA's statutory framework.[119] The IPT found that no legislation had served to repeal or override section 94 since its passage as law. The ITP reached that conclusion by finding that nothing within the text of section 80 of RIPA should be construed as prejudicing any lawful power to obtain information in ways not specified by RIPA.[120] In exploring what a lawful collection regime under section 94 would look like, the ITP focused heavily on the foreseeability of interferences with privacy,[121] evaluating what is reasonable when the government acts in the interests of national security, without requiring measures to the extent that any individual can predict whenever authorities are likely to acquire his or her communications data.[122] The GCHQ had been in breach of this foreseeability requirement by its use of section 94 to collect bulk communications data for over a decade, as it used the loopholes in this decades-old statute to engage in modern data gathering practices.[123] The ITP ultimately decided, however, that recent safeguards put into place, as well as newfound

115. *Id.* at [97]–[101].
116. *Id.* at [96]–[97].
117. [2015] H.R.L.R. 2, [114].
118. *Id.*
119. [2016] H.R.L.R. 21, [26].
120. *Id.* at [40].
121. *Id.* at [59], [70].
122. *Id.*
123. *Id.* at [59], [70].

public awareness of the section 94 regime, sufficed to find the GCHQ within the bounds of Article 8.[124]

III. THE ARTICLE 10 ENCODED FREEDOM OF JOURNALISTIC EXPRESSION

Alongside the jurisprudence surrounding electronic surveillance, Article 10 also covers the right to journalistic freedom of expression. This Part will delve into the damage that the GCHQ's collection of metadata has on journalistic freedom of expression under Article 10. It will analyze the government interest of national security against the interference of journalistic expression as components of what is necessary in a democratic society. It will then weigh the claims of an overriding national security interest made by proponents of the collection of metadata with a counterargument to those claims, which undercuts the effectiveness of metadata collection as an effective method of preventing public harm. It will also briefly examine Article 10 itself and how the freedom of journalistic expression is a necessary pillar of a democratic society. This Part will then demonstrate how metadata collection, such as that done by the GCHQ, stifles expression by interfering with journalists' ability to procure anonymous sources. Finally, this Part will demonstrate how metadata collection also stifles journalistic expression by creating a chilling effect that interferes with journalists' ability to freely express controversial ideas, which the public may need to hear.

A. The Alleged Necessity of Metadata Collection in the Interests of National Security

Supporters of metadata collection argue that it is a justifiable potential infringement on Article 8 and 10 rights, since protection of national security is a legitimate government aim and necessary in a democratic society.[125] The Intelligence and Security Agencies of Britain exist and justify their existence, in large part, to protect the country from breaches of national security

124. *Id.* at [94].

125. Intelligence and Security Committee of Parliament, Privacy and Security: A Modern and Transparent Legal Framework, 2015, HC 1075, ¶ 10 [hereinafter Committee Report]; Freedom of Expression in Europe, *supra* note 17 at 7–10.

through the use of their intelligence gathering programs.[126] Supporters of metadata collection claim that metadata is essential for agencies' abilities to develop leads on dangerous individuals and to identify potentially dangerous associations or networks of communication.[127] These mechanisms of identification, it is argued, are more vital in this age, as growing terrorist threats may be preempted through communications data identification.[128] Much is made of the fact that, in a world where these threats must be identified, metadata acquisition is at least less intrusive than the interception of content data.[129] Some consider an approach to surveillance that affords greater respect to privacy and expression to be misguided.[130] Arguments with much force come out of the enormous cost of individual terrorist attacks when compared against the seemingly less tangible cost of intrusions upon privacy or expression.[131]

These arguments heralding the strength of the relevant national security interests have, however, been met with criticism.[132] There are those who have pointed to the ongoing march of technology as cause for an erosion of the distinction between metadata, which has less procedural protections, and content data, which has more.[133] Communications data in the internet age can create a nearly complete profile of an individual's life.[134] While some argue the difference between metadata and content data is still meaningful, they also must deal with the wide and sweeping nature of metadata acquisition.[135] Experts contend that sweeping surveillance techniques, such as communications data acquisition, produce wide and deep privacy intrusions, with far less of a security benefit than targeted surveillance.[136] Research suggests that mass collection of communications data is not only ineffective at preventing individual acts of terror, but

126. Committee Report, *supra* note 125, ¶ 13.
127. *Id.* ¶ 10.
128. *Id.* ¶ 10.
129. *Id.* ¶ 140.
130. Epstein, s*upra* note 19, at 332–33.
131. *Id.* at 330–34.
132. *See* Martin Scheinin, *Towards Evidence-Based Discussion on Surveillance: A Rejoinder to Richard A. Epstein*, 12 E.C.L. REV. 341, 347–48 (2015).
133. Committee Report, *supra* note 126, ¶ 50.
134. *Id.* ¶¶ 130, 138.
135. Scheinin, *supra* note 132.
136. *Id.*

that collection of an abundance of noncontent data can mislead law officers and even obfuscate proper leads.[137]

B. Journalistic Expression is a Recognized Pillar of a Democratic Society

The ineffective form of security procured through metadata collection is outweighed by the countervailing interest of journalistic expression. Article 10 of the ECHR is a guarantee to the people of those nations that accede to the ECHR that their right to express themselves will be protected above and beyond the authority of the sovereign state in which they live.[138] These principles were considered so sacrosanct by the international community that, in the aftermath of the Snowden leaks, the United Nation's Human Rights Council declared that:

> In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous. Privacy of communications infers that individuals are able to exchange information and ideas in a space that is beyond the reach of other members of society, the private sector, and ultimately the State itself. Security of communications means that individuals should be able to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion. Anonymity of communications is one of the most important advances enabled by the Internet, and allows individuals to express themselves freely without fear of retribution or condemnation.[139]

In response to this, the United Nations General Assembly passed Resolution 68/167, which stresses, in part, "the im-

137. Committee Report, *supra* note 125, ¶ 137; Scheinin, *supra* note 132.

138. ECHR Art. 10, *supra* note 8.

139. Frank La Rue (Special Rapporteur), *Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/17/27 (May 16, 2011). The United Nation's Human Rights Council is a branch of the U.N. General Assembly, comprised of forty-seven U.N. Member States and charged with overseeing human rights issues, including the strengthening of existing human rights protections and the resolution of present human rights violations. *About The Human Rights Council*, U.N. HUM. RTS. OFF., http://www.ohchr.org/en/hrbodies/hrc/pages/hrcindex.aspx, (last visited Jan. 16, 2017).

portance of the full respect for freedom to seek, receive and impart information, including the fundamental importance of access to information and democratic participation."[140]

One also need not look very hard to find that the integrity of journalistic freedom of expression is both logically and historically bound to the greater right of expression, which is treasured in these and other declarations of human rights.[141] Those nations across the globe who hold themselves to democratic principles often hold freedom of the press as the epitome of the values of open communication and discourse.[142]

The First Amendment of the U.S. Constitution also expressly provides that, "Congress shall make no law . . . abridging the freedom of speech, or of the press. . . ."[143] The U.S. Supreme Court has applied the First Amendment to protect the right of citizens to freely express themselves,[144] as well as the right of the

---

140. G.A. Res. 68/167, pmbl., The Right to Privacy in the Digital Age (Jan. 21, 2014). The United Nations depicts its own history and mission statement as follows:

> Established in 1945 under the Charter of the United Nations, the General Assembly occupies a central position as the chief deliberative, policymaking and representative organ of the United Nations. Comprising all 193 Members of The United Nations, it provides a unique forum for multilateral discussion of the full spectrum of international issues covered by the Charter. It also plays a significant role in the process of standard-setting and the codification of international law. . . . The Assembly is empowered to make recommendations to States on international issues within its competence. It has also initiated actions—political, economic, humanitarian, social and legal—which have affected the lives of millions of people throughout the world.

Functions and Powers of the General Assembly, UNITED NATIONS, http://www.un.org/en/ga/about/background.shtml (last visited Jan. 16, 2017).

141. Filipov, *supra* note 13 at 64–83.

142. *Id.*

143. U.S. CONST. amend. I.

144. While the word "expression" is not explicitly found within the First Amendment, the U.S. Supreme Court has found a First Amendment right to express oneself, not merely within the confines of the spoken word, but where one asserts their viewpoints into the public discourse. *See* Barry P. McDonald, *The First Amendment and the Free Flow of Information: Towards A Realistic Right to Gather Information in the Information Age*, 65 OHIO ST. L.J. 249 (2004). *See, e.g.*, Texas v. Johnson, 491 U.S. 397 (1989) (striking down a Texas

press to communicate ideas effectively without undue interference from the government.[145]

The Committee of Ministers of the Council of Europe also adopted Recommendation No. R (2000) 7, a recommendation to the Member States of the European Union, which states that journalists have a right not to disclose their sources of information.[146] Principle 6 of the Recommendation, in particular, applies to interception orders, actions concerning communications or correspondence, and surveillance orders concerning journalists, their contacts, or their employers.[147] It states that those methods cannot be undertaken where, "[t]heir purpose is to circumvent the right of journalists . . . not to disclose information identifying a source."[148]

It is also evident in the ECtHR's case law that Article 10 places a premium on journalistic freedom of expression.[149] In *Özgür Gündem*, the Turkish government was found to be in violation of Article 10 of the ECHR, as it failed to conduct a widespread investigation into a concerted campaign of serious attacks against journalists and others associated with a newspaper company.[150] The ECtHR ruled that the freedom of journalistic expression was of such significance that it could require a country to do more than merely refrain from interfering with said

---

statute banning a person's right to burn a flag); Buckley v. Valeo, 424 U.S. 1 (1976) (upholding a person's right to contribute money to political campaigns based on a First Amendment right to express oneself, not merely within the confines of the spoken word, but where one asserts their viewpoints into the public discourse).

145. *See, e.g.*, N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964) (holding that in order for a statement printed by the press about a public figure to be found illegal under a theory of libel, the statement must be made with actual malice, or purposeful intent to print a false statement); N.Y. Times v. United States, 403 U.S. 713 (1971) (holding that the publication of classified documents about the Vietnam War could not be suppressed under a government theory of national security).

146. Council of Europe, Committee of Ministers, Recommendation No. R (2000) 7, Of the Committee of Ministers to Member States on the Right of Journalists Not to Disclose Their Sources of Information (Adopted by the Committee of Ministers at the 701st Meeting of the Ministers' Deputies on March 8, 2000).

147. *Id.*

148. *Id.*

149. Filipov, *supra* note 13, at 66.

150. *Özgür Gündem*, 31 Eur. H.R. Rep. 49, 1086–87 (2000).

right.[151] There, the Court found an obligation for states to take positive action to investigate serious allegations that legal authorities may be engaging in interferences with journalistic freedom of expression.[152] *Telegraaf Media Nederland Landelijke Media BV* is a more recent case that highlights the respect with which the ECtHR gives the freedom of journalistic expression.[153] The ECtHR cited legislative declarations, such as Recommendation No. R (2000) 7, declaring that confidential sources are so essential to Article 10 principles that there must be an overriding requirement to the public interest in order to take measures that would breach that confidentiality.[154]

C. Metadata Collection is at Odds with Journalists' Need for Anonymous Sources

One of the key components of modern investigative journalism is a reporter's ability to access confidential informants.[155] The routine disclosures of confidential sources with particular insight into the nature of both government and nongovernment organizations are essential to a reporter's role within the democratic exchange of information.[156] "Off the record," deliberate drops from low-level sources can be mandated from higher ups within-organizations.[157] There are records of government actors within each branch and on every level of the chain of command who leak information, ranging from arbitrary gossip to earth-shattering news.[158] Anonymous source disclosures are of such a

151. *Özgür Gündem*, 31 Eur. H.R. Rep. 49, 1083 (2000).

152. *Id.*

153. 34 B.H.R.C. 193 at [60]–[62], [98]–[100], [126]–[128] (2012); http://hudoc.echr.coe.int/eng?i=001-114439.

154. *Id.* at [60]–[62].

155. *See* Michelle C. Gabriel, *Plugging Leaks: The Necessity of Distinguishing Whistleblowers and Wrongdoers in the Free Flow of Information Act*, 40 LOY. UNIV. CHI. L. REV. 531 (2009); *Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy*, HUM. RTS. WATCH (2014), https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and; Bell et al., *supra* note 14; Mădălina Ciobanu, *Research Highlights the Impact of the Threat of Surveillance on Journalists and Their Sources*, JOURNALISM.CO.UK (May 31, 2016), https://www.journalism.co.uk/news/research-highlights-the-impact-of-the-threat-of-surveillance-on-journalists-and-their-sources/s2/a642711/.

156. *See* Bell et al., *supra* note 14.

157. *Id.* at 2.

158. *Id.* at 2.

common occurrence and are so vital to the press in the United States that forty states have shield law statutes that provide protections for anonymous sources.[159] Nine states that do not have shield laws instead have standing court rulings that protect anonymous disclosures through the common law system.[160]

In a world after the Snowden leaks, potential sources in the United States, United Kingdom, and other countries worldwide, are now discouraged from coming forth and providing information to journalists.[161] A comprehensive survey by the Human Rights Watch and ACLU revealed that the loss of sources is a prominent concern amongst American journalists.[162] Journalists

---

159. Forty states in the United States now have anonymous source protection laws, known as "shield laws," as a part of their state code. Gabriel, *supra* note 155, at 531–32; *State-by-State Guide to the Reporter's Privilege For Student Media*, STUDENT PRESS L. CENTER, http://www.splc.org/article/2010/09/state-by-state-guide-to-the-reporters-privilege-for-student-media?id=60 (last visited Jan. 16, 2017) [hereinafter *State-by-State Guide*].

160. Nine states in the United States have state courts who, through the common law system, have created protections for anonymous sources without having any shield laws in their code. Wyoming is the only state in the union to have neither a shield law statute nor a common law developed First Amendment protection for confidential sources. *See* Gabriel, *supra* note 155; *State-by-State Guide*, *supra* note 159. *See, e.g.*, In re Wright, 700 P.2d 40 (Idaho 1985); Waterloo/Cedar Falls Courier v. Hawkeye Community College, 646 N.W.2d 97 (Iowa 2002); Sinnott v. Boston Retirement Board, 524 N.E.2d 100 (Mass. 1988); Hawkins v. Williams, Civ. No. 2900054 (Cir. Ct. 1st Jud. Dist. Hinds Cty., Mar. 16, 1983); Mississippi v. Hardin, Crim. No. 3858 (Cir. Ct. Yalobusha Cty., Mar. 23, 1983); State of Missouri v. Ely, 954 S.W.2d 650 (Mo. Ct. App. W.D. 1997); New Hampshire v. Siel, 444 A.2d 499 (N.H. 1982); Hopewell v. Midcontinent Broadcasting Corporation, 538 N.W.2d 780 (S.D. 1995); State v. St. Peter, 132 Vt. 266 (1974); Brown v. Commonwealth of Virginia, 204 S.E.2d 429 (Va. 1974).

161. *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy*, HUM. RTS. WATCH (July 28, 2014), https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and [hereinafter *With Liberty to Monitor All*]; Ciobanu, *supra* note 155.

162. *With Liberty to Monitor All*, *supra* note 161. The Human Rights Watch is a nongovernmental, international organization whose mission statement is, in their own words, to "scrupulously investigate abuses, expose the facts widely, and pressure those with power to respect rights and secure justice. Human Rights Watch is an independent, international organization that works as part of a vibrant movement to uphold human dignity and advance the cause of human rights for all." *About Us*, HUM. RTS. WATCH, https://www.hrw.org/about (last visited Oct. 1, 2017). They neither accept government funding in any form nor do they purport to identify with any partisan group or political party. *Id.* The Human Rights Watch receives praise for its

in the survey cited a myriad of potential reasons for the newfound difficulty in procuring sources.[163] The most common reason given was the increased surveillance and thorough crackdown on journalistic whistle-blowers through the use of the Espionage Act in the Obama Administration.[164] Beyond the Obama Administration's now liberal use of its own discretion in prosecuting sources who fail to comport with the alleged national security interest, journalists noted that electronic surveillance now made the discovery of those sources' identities much easier for the government.[165] The government could potentially be observing where and when a source was in a given place by storing and analyzing metadata regarding phones, electronic building identifications, and publicly used surveillance cameras in concert.[166]

Journalists now complain that both they, and their sources, can assume that their every move is potentially under scrutiny from the government.[167] Sources will request to specifically meet with reporters in their own homes, as opposed to public offices.[168]

---

journalism and investigatory abilities, despite not operating under the purview of traditional news media organizations. Dan Gilmor, *In Praise of The Almost Journalists*, SLATE (Mar. 28, 2014), http://www.slate.com/articles/technology/future_tense/2014/03/human_rights_watch_and_other_advocacy_groups_doing_great_journalism.html.

163. *With Liberty to Monitor All*, *supra* note 161.

164. *Id.* The U.S. Executive Branch, under president Barack Obama, has been infamously harsh on administrating punishment for those individuals who expose classified information in the perceived interest of rooting out government corruption, abuse, and wrongdoing under the Espionage Act of 1917. Gunar Olsen, *Obama's Crackdown on Whistleblowers: Petraeus Plea Deal Reveals Double Standard for Leaks*, HUFFINGTON POST (Apr. 22, 2015), http://www.huffingtonpost.com/gunar-olsen/obamas-crackdown-on-whist_b_7109518.html. The Espionage Act of 1917 was passed by U.S. President Woodrow Wilson during World War I for the purpose of imposing harsh punishments on those individuals who leaked government information that could be used by German forces in their war effort. Gunar Olsen. *Id.*; *This Day in History—June 15, 1917: U.S. Congress Passes Espionage Act*," HISTORY, http://www.history.com/this-day-in-history/u-s-congress-passes-espionage-act (last visited Jan. 16, 2017). Violating the Act is a strict liability offense, meaning those found to have definitively been in breach of it cannot mount any defense. *Id.*

165. *With Liberty to Monitor All*, *supra* note 161.

166. *Id.*; Stratford, *supra* note 3, at 132; Bell et al., *supra* note 14, at 14.

167. Bell et al., *supra* note 14 at 10–11.

168. *With Liberty to Monitor All*, *supra* note 161; Bell et al., *supra* note 14, at 14.

Journalists are changing their reporting practices to account for the fact that they can no longer confirm even unclassified information, such as the previously mentioned routine disclosures.[169]

D. Metadata Collection Stifles Journalistic Expression Through a Collective Chilling Effect

Government interception of surface data serves to stifle the journalists who use electronic communications pathways in order to not only procure information, but to convey that information to the public.[170] The idea that government surveillance has a tangible chilling effect on free expression is nothing new.[171] Proving that the chilling effect exists presents definite problems of empirical proof, as it is an exercise in proving the nonexistence of an action—free expression.[172] With the Snowden revelations, as well as the accompanying international discussion on the nature of government surveillance, researchers are now pushing surveys in order to supply some tangible data to either prove or disprove the existence of a chilling effect for both journalists and laypersons.[173]

---

169. *With Liberty to Monitor All*, *supra* note 161; Bell et al., *supra* note 14, at 14.

170. *With Liberty to Monitor All*, *supra* note 161; Bell et al., *supra* note 14, at 11–12.

171. *See e.g.*, Laird v. Tatum, 408 U.S. 1 (1972) (dismissing the plaintiff's complaint that the U.S. military data-gathering systems chilled their speech in violation of their First Amendment rights, reasoning that the plaintiff's failed to establish standing); Klass v. Federal Republic of Germany, 2 Eur. H.R. Rep. 214 (1978) (holding that although plaintiffs had not been specifically wiretapped by the German government, their complaint could validly ask for an evaluation of the German surveillance system as relief because the nature of the surveillance system was so widespread that they had the standing to do so); Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L. J. 118, 120 (2016).

172. Penney, *supra* note 171. It is worth noting the counterargument against the proposition that proving a negative has an inherent difficulty which distinguishes it from the task of proving a positive proposition. *See* Kevin W. Saunders, *The Mythic Difficulty in Proving a Negative*, 15 SETON HALL L. REV. 277, 277 (1985). It has been posited that the difficulty in proving negative propositions can stem from other characteristics of the proposition to be proven, such as the universality or rarity of those characteristics. *Id.*

173. For one example of a thorough study of individual's online activities and how they are markedly changed by the existence of government surveillance systems, see Penney, *supra* note 171.

The atmosphere created by government surveillance has a tangible effect on how writers and journalists around the world view their freedom of expression.[174] Levels of writers'[175] discomfort with government surveillance is nearly as high in liberal democratic, "free"[176] countries as it is in nondemocratic countries with histories of state surveillance.[177] Writers in the five nations that comprise the "Five Eyes" countries, one of which is the United Kingdom, particularly share this heightened level of concern.[178]

---

174. A 2015 survey conducted by the PEN American Center polled writers living in fifty different countries to gauge how government surveillance influences their attitudes towards freedom of privacy and expression, as well as how those attitudes effect their journalistic practices. *See* PEN AM. CENTER, *supra* note 14.

175. The term "writers" is defined in the PEN report based on how the respondents chose to style themselves. PEN AM. CENTER *supra* note 14, at 7. This report included fiction, nonfiction, academic, creative, and journalistic sources. *Id.*; *see Methodology, Freedom in the World (2015)*, FREEDOM HOUSE https://freedomhouse.org/report/freedom-world-2015/methodology (last visited Jan. 16, 2017).

176. *See Methodology, Freedom in the World (2015)*, *supra* note 175.

177. Of the 772 respondents, 82 percent described themselves as writers, and of that group, 22 percent described themselves as journalists. PEN AM. CENTER, *supra* note 14, at 7. The term "free" is defined in the PEN report as those countries that qualify as liberal democracies by the criteria of Freedom House, which is a nongovernmental watchdog organization. *See Methodology, Freedom in the World (2015)*, *supra* note 175. Freedom House grades countries on seven criteria—electoral process, political pluralism and participation, functioning of government, freedom of expression and belief, associational and organizational rights, rule of law, and personal autonomy and individual rights—and finds them as free, partly free, or not free. *Id.* PEN report showed that writers in 75 percent of those countries classified as "free," compared to 84 percent of writers in those countries classified as "partly free," and 80 percent of those "not free" countries were either very or somewhat worried about levels of government surveillance in their own countries. PEN AM. CENTER, *supra* note 14, at 22.

178. As depicted in a synopsis by Privacy International:

> The Five Eyes alliance is a secretive, global surveillance arrangement of States comprised of the United States National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), Canada's Communications Security Establishment Canada (CSEC), the Australian Signals Directorate (ASD), and New Zealand's Government Communications Security Bureau (GCSB). . . . Under the agreement interception, collection, acquisition, analysis, and decryption is conducted by each of the State parties

Writers in "free" countries are now more apt to avoid speaking, writing, or conducting research on a certain topic for fear of surveillance and its accompanying consequences.[179] In accordance with a fear of government surveillance, writers steer clear of certain topics in phone conversations or email messages, while also refraining from conducting internet searches or visiting certain websites.[180] Journalists, in particular, will employ encryption technology for their correspondences.[181] Those who employ less advanced methods will deliberately create a misleading electronic trail, or even discard the use of electronic communications entirely for information of great import.[182]

> in their respective parts of the globe, and all intelligence information is shared by default.

What is the Five Eyes?, PRIVACY INT'L, https://www.privacyinternational.org/node/51 (last visited Jan. 16, 2017). Of the 772 writers surveyed in the PEN study, 171, or approximately 22 percent, lived in the "Five Eyes" countries. PEN AM. CENTER, *supra* note 14, at 22. 22 percent of writers within that sample lived in the United Kingdom at the time of the survey. *Id.* 84 percent of writers in the "Five Eyes" alliance countries report that they are either very or somewhat worried about government surveillance. *Id.*

179. The PEN report showed that 34 percent of writers in free countries either avoided writing on a particular topic, or have considered failing to write on that topic. *Id.* Compare this with 27 percent of U.S. writers, who reported the same in a 2013 PEN survey. *Id.*

180. 34 percent of writers in free countries have avoided certain topics in their personal phone calls and email messages, or at least seriously considered it. *Id.* at 10. 42 percent of writers living in free countries have refrained from conducting internet searches and visiting websites that may be considered controversial, or at least seriously considered refraining from such activities. *Id.* at 10.

181. Whether encryption is efficient or effective is another story entirely, as the Human Rights Watch and ACLU report explains that, "[a] significant number of journalists reported using various forms of encryption software for their communications with sources or colleagues, including emails, chats, texts, and phone calls, though it is far from clear how effective these methods are in the long run." *With Liberty to Monitor All*, *supra* note 161.

182. Journalists will, for example, call many misleading and unrelated sources before a big story is about to drop in an attempt to mislead any potential data collection systems *Id*. at 36. Journalists who are weary of data collection and tracking are also more likely to prefer phone calls to emails, to prefer landline phone calls to cell phone calls, and to prefer in-person meetings with sources to any of the former. *Id*. at 36.

IV. A MORE THOROUGH REVIEW OF U.K. SURVEILLANCE LAW

The wide reaching nature of the GCHQ's surveillance operations, the contested nature of national security as a legitimate government interest, and the damage done to journalistic freedom of expression all highlight that the current approach to communications data acquisition is either poorly executed or fundamentally misguided.[183] In order to provide a remedy for the systemic problems that egregiously alter journalistic behavior, there must be systematic solutions.[184] The answer is a three-part solution that attacks the issue on several fronts. First, the legislative framework of metadata collection in the United Kingdom, with its reliance on now decades-old provisions, must be brought under fundamental review by the British Parliament.[185] This would entail a top-down analysis of the laws, including those that have been misused, and a revamp of the legislative scheme surrounding electronic surveillance. Section 94 was passed in an era before modern internet existed, RIPA was passed amidst debate and criticism, and both provisions were passed before metadata could physically trace journalists and their sources.[186] The statutory framework demands more than just an update to be in compliance with Article 10's guarantee of freedom of expression.[187] This argument is only strengthened by the fact that the GCHQ had been using the section 94 regime unlawfully for nearly a decade.[188]

Second, because Article 8's right to privacy linked inextricably both to Article 10's freedom of expression and the damage done by metadata collection, any new surveillance system must align with a new philosophy towards an individual right to privacy.[189] Scholars and legal authorities on both sides of the Atlantic have contemplated the very real possibility that traditional notions of

183. *See* Donohue, *supra* note 51, at 1059; Bell et al., *supra* note 14, at 13; *see also With Liberty to Monitor All*, *supra* note 161.

184. *See With Liberty to Monitor All*, *supra* note 161.

185. *See* Rafi Azim-Khan & Steven P. Farmer, *The U.K. Government's Draft Codes to Clarify New Legislation on Communications Data Retention and Investigatory Powers*, PILLSBURY LAW (Feb. 28, 2015), http://www.pillsburylaw.com/publications/the-uk-governments-draft-codes-to-clarify-new-legislation-on-communications-data-retention-and-investigatory-powers.

186. *See* Committee Report, *supra* note 125, ¶ 136.

187. *Id.*

188. *See Privacy International* [2016] H.R.L.R. 21.

189. Donohue, *supra* note 51, at 1200–01.

privacy rights may be ill-equipped to keep up with the ongoing improvement of technology.[190] Those who argue the disappearing line between content data and metadata acknowledge this, and ask whether there is a meaningful difference between the two in an age where individuals constantly interact with others through internet and phone communications, and journalists rely on these communications to keep up with the pace of society.[191] A personal privacy right in one's data would mandate greater care on the part of any government official who sought to use this data, and also a personal right on behalf of the individual, so that he or she may challenge the theft or misuse of his or her data in court.[192] This would at least provide journalists with a direct method to challenge the taking of their information, as well as assuage the fears of journalists and sources that their personal information will be up for grabs.[193]

Finally, any new metadata acquisition program should mandate judicial oversight for any applications for authorization to collect communications data from journalists and other officials who hold privileged information.[194] This removes the grey area for authorization applicants to decide, before authorization from a judge, whether the relevant data is likely to fit within the Code of Practice's new procedural guidelines for communication data, which would be for the express purpose of exposing confidential sources.[195] It is these grey areas where there is the most room for abuse and error within agencies, such as the GCHQ.[196] Removal of such chance of abuse and error would serve to ease the burden on journalists and their sources and allow for preservation of freedom of expression.[197]

---

190. *Id.*; *see also* U.S. v. Jones, 565 U.S. 400, 413–31 (2012) (Sotomayor, J., concurring) (discussing the inadequacy of the legal methodologies around the protection of privacy in a modern society, where the rapid pace of technology allows government actors easy access to more of citizens' personal information).

191. Committee Report, *supra* note 125, ¶¶ 136–37; Donohue, *supra* note 51, at 1140–41; *With Liberty to Monitor All*, *supra* note 161.

192. Donohue, *supra* note 51, at 1200–01.

193. Bell et al., *supra* note 14, at 13.

194. *See* Azim-Khan & Farmer, *supra* note 185.

195. HOME OFF., *supra* note 61, at 45–48.

196. *Regulation of Investigatory Powers Act 2000*, *supra* note 46.

197. Bell et al., *supra* note 14, at 13; *see also With Liberty to Monitor All*, *supra* note 161.

CONCLUSION

In a digital world, journalists must remain free to compile information from sources and to express that information for the good of society. Where governments can use metadata collection to trace journalists' activities, those journalists are stifled in their ability to express themselves.[198] Nations come together and accede to international conventions, like the ECHR, to protect fundamental democratic principles like freedom of expression.[199] In order to comport with ECHR Article 10's guarantee of freedom of expression, it is necessary that the statutory framework under which the GCHQ operates ensures that it does not stifle the activities of journalists.[200] The three-part solution put forth by this Note can be a big step forward towards a more workable formulation of British surveillance. It is only when the U.K.'s government revamps its legislation, changes its philosophical views on privacy, and tightens its administrative safeguards, that the GCHQ's collection of metadata will align with the principles and text of Article 10 of the ECHR.[201]

Matthew B. Hurowitz[*]

198. *See With Liberty to Monitor All*, *supra* note 161.

199. Freedom of Expression in Europe, *supra* note 17, at 7.

200. *See* ECHR Art. 10, *supra* note 8.

201. *Id.* This article was completed in January 2017. Several developments have occurred between that time and the journal going to press in late 2018. As these events are ongoing, their consequences are not yet clear.

* B.A., State University of New York at Binghamton; J.D., Brooklyn Law School (Expected 2018); Executive Notes & Comments Editor, *Brooklyn Journal of International Law* (2017–2018). I would like to thank the staff of the *Brooklyn Journal of International Law* for all their work in the publication of my Note. I would like to give a special thanks to Jessica Martin and Michelle Lee, whose great efforts and generous help made the publication process significantly easier. I would also like to thank my parents, Janice and Charles Hurowitz, for being the giants upon whose shoulders I stand. None of this would be possible without their love and support. All errors or omissions are my own.