Washington University Global Studies Law Review

Volume 17 | Issue 3

2018

Intelligence-Sharing Agreements & International Data Protection: Avoiding a Global Surveillance State

Rachel C. Taylor

INTELLIGENCE-SHARING AGREEMENTS & INTERNATIONAL DATA PROTECTION: AVOIDING A GLOBAL SURVEILLANCE STATE

I. INTRODUCTION

In 2013, the trust between the American public and its government was broken,[1] resulting in "a sea change in the policy landscape related to surveillance."[2] Because of the Snowden disclosures, the American intelligence community was forced into a dialogue with the public and began trading security for domestic legitimacy.[3] However, this conversation is not only of domestic concern.[4] As national security continues to focus on international threats, international solutions and approaches to threats must be implemented. Globally, individual privacy concerns prompted significant movement among data protection rights and legislation post-Snowden.[5] Democratic norms demand transparency and oversight for the intelligence community.[6] While this note touches on citizens' concerns in protecting their data privacy from unchecked national surveillance regimes, its primary focus is in maintaining the integrity of

1 *See generally* Marcy Wheeler, *Government Spying: Why You Can't 'Just Trust Us,'* NATION (Jun. 19, 2013), https://www.thenation.com/article/government-spying-why-you-cant-just-trust-us/; Timothy B. Lee, *Here's why 'Trust Us' Isn't Working for the NSA Any More*, WASH. POST (Jul. 30, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/07/30/heres-why-trust-us-isnt-working-for-the-nsa-any-more/?utm_term=.8fee9542b2f5.

2 Rainey Reitman, *3 Years Later, the Snowden Leaks Have Changed How the World Sees NSA Surveillance*, ELEC. FRONTIER FOUND. (Jun. 5, 2016), https://www.eff.org/deeplinks/2016/06/3-years-later-snowden-leaks-have-changed-how-world-sees-nsa-surveillance.

3 Jack Goldsmith, *Three Years Later: How Snowden Helped the U.S. Intelligence Community*, LAWFARE (Jun. 6, 2016, 9:32 AM), https://www.lawfareblog.com/three-years-later-how-snowden-helped-us-intelligence-community.

4 *See Global Opposition to USA Big Brother Mass Surveillance*, AMNESTY INT'L (Mar. 18, 2015), https://www.amnesty.org/en/press-releases/2015/03/global-opposition-to-usa-big-brother-mass-surveillance/ (detailing global public opposition to the Unites States' surveillance practices); *see also* David Miranda & Joseph Huff-Hanon, *Edward Snowden Inspires Global Treaty for Online Privacy*, ROLLING STONE (Sept. 24, 2015), http://www.rollingstone.com/politics/news/edward-snowden-inspires-global-treaty-for-online-privacy-20150924 (discussing the drafting of an international treaty to deal with post-Snowden privacy concerns).

5 *See, e.g.*, EUROPEAN COMM'N, Q&A: GUIDANCE ON TRANSATLANTIC DATA TRANSFERS FOLLOWING THE SCHREMS RULING 1 (2015), http://europa.eu/rapid/press-release_MEMO-15-6014_en.htm.

6 Elizabeth Sepper, *Democracy, Human Rights, and Intelligence Sharing*, 46 TEX. INT'L L. J. 151, 166 (2011).

domestic safeguards by pushing against secret intelligence-sharing agreements that sidestep national laws. This note examines legal challenges that dismantle and change the international surveillance framework.

Part II discusses the Five Eyes alliance and intelligence-sharing relationships between states participating in the information-sharing agreement, particularly the United States and the United Kingdom, in a post-Snowden world. Part II also reviews laws within these nations that relate to intelligence-gathering and sharing. Germany is also discussed in Part II, contrasting its role as a Western ally but not as a Five Eyes partner. Part III considers the Privacy Shield and European courts' response to national security justifications in *Schrems I*. Part IV draws lessons from *Schrems I* and the European Union's data protection regime, and proposes that American lawmakers and judges take greater responsibility in overseeing the U.S. intelligence community, evinced by the excessive deference these two branches afford to the Executive Branch as an obstacle to democratic governance. Finally, this note concludes by encouraging greater congressional engagement with data protection issues, including national security concerns and government surveillance, given the threat posed by globalized threats to national security.

II. THE FIVE EYES

While the Five Eyes agreement is one of the more famous intelligence-sharing agreements, there are other partnerships and less formal means of collaboration.[7] Often, the exchange of intelligence depends on the health of the relationship between collaborating parties and the historical level of cooperation.[8] All of these intelligence-sharing relationships depend on trust—trusting the veracity of the information, its confidentiality, and the sensitivity with which the receiving party demonstrates in handling the information.[9] Breaches of trust in these intelligence-sharing relationships exacerbate the inherent tensions residing in cooperative espionage.[10] As previously discussed, the impact of the

7 Scarlet Kim, et al., *The "Backdoor Search Loophole" Isn't Our Only Problem: The Dangers of Global Information Sharing*, JUST. SEC. (Nov. 28, 2017), https://www.justsecurity.org/47282/backdoor-search-loophole-isnt-problem-dangers-global-information-sharing/.

8 Priscilla Alvarez, *The Risks of Sharing Intelligence*, ATLANTIC (May 16, 2017), https://www.theatlantic.com/politics/archive/2017/05/trump-russia-intelligence-sharing/526857/.

9 *See* Sepper, *supra* note 6, at 162.

10 INTERNATIONAL INTELLIGENCE COOPERATION AND ACCOUNTABILITY 23 (Hans Born et al.

various leaks between the U.S. and its partners have corroded the trust underlying these intelligence-sharing alliances.[11] The greater threat to the status quo surrounding the intelligence community, however, is the onset of litigation that attacks the global infrastructure facilitating the streams of information between allied states.[12] This note discusses the circumvention of states' own domestic protections against unauthorized surveillance and data collection through such agreements.

Governments do not collect information solely for their own local use. Information-sharing between allied states with similar interests and threats is an established practice that should shape the debate around government surveillance. There is potential that information collected in the U.S. will be circulated beyond the American border. In 1946, a series of bilateral intelligence sharing agreements between five English-speaking countries developed into the UKUSA agreement – now known as the Five Eyes alliance.[13] This post-war alliance established a global surveillance infrastructure to observe the world's communications, internationally and domestically.[14] Besides the United States, the four other countries are Australia, United Kingdom, Canada, and New Zealand—nations that are unaffected by the First Amendment.[15] While the crux of these agreements

---

eds., 2011). "[I]ntelligence suffers from a paradox - it is only valuable when shared with those who need it, but the more it is shared the more it risks being compromised, and the lower its value." Janine McGruddy, *Multilateral Intelligence Collaboration and International Oversight*, 6 J. OF STRATEGIC STUD. 214, 215 (2013).

11 Henry Overton, *The Five Eyes in the Trump era: Dominant or Diminished?*, FOREIGN BRIEF (July 7, 2017), http://www.foreignbrief.com/united-states/five-eyes-trump-era-dominant-diminished/. "The leaks from Washington could very well justify changes to the processes of intelligence sharing between the Five Eyes members in the same way that Trump's disclosure of sensitive information gathered by Israel caused the country to 'tweak' its intelligence sharing protocols with the US." *Id*. *See also* Alvarez, *supra* note 8.

12 This note discusses several cases that look to expose the secret information-sharing agreements that intensify the "accountability gap" present in the intelligence community. INTERNATIONAL INTELLIGENCE COOPERATION AND ACCOUNTABILITY, *supra* note 10, at 90-91 (defining "accountability gap" as "a failure by review bodies to keep pace with international cooperation between intelligence services").

13 *The Five Eyes Fact Sheet*, PRIVACY INT'L (Nov. 26, 2013) https://www.privacyinternational.org/blog/1204/five-eyes-fact-sheet.

14 *Id.*

15 *Id*. In March 1946, the UKUSA agreement was brokered between the United States and Great Britain. The deal was then extended to Canada "in 1948, and Australia and New Zealand in 1956." Richard Norton-Taylor, *Not So Secret: Deal at the Heart of UK-US Intelligence*, GUARDIAN (Jun. 24, 2010), https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released. The Five Eyes partners do often join up with other countries. J. Vitor Tossini, *The Five Eyes – The Intelligence Alliance of the Anglosphere*, UK DEF. J. (Nov. 14, 2017), https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/ ("[T]he co-operation with Denmark, France, Norway and the Netherlands receives the name of 'Nine Eyes', and there is the 'Fourteen Eyes' which consists of the previously mentioned Nine Eyes plus Belgium, Germany, Italy, Spain and Sweden.")

is to collaborate on international crime, there is evidence that these nations' respective intelligence agencies have conducted domestic surveillance circumventing their local, legal safeguards.[16]

A. The United States

In the United States, private technology companies can be forced to provide users' data through National Security Letters ("NSLs") or the Foreign Intelligence Surveillance Act ("FISA") for national security investigations.[17] These orders come with a nondisclosure provision that muzzle the recipient from disclosing that they were forced to pass this information along to the government.[18] FISA orders were created with the passage of Foreign Intelligence Surveillance Act in 1978. [19] The law determined that "non-criminal electronic surveillances within the United States were only permissible for collecting foreign intelligence and/or foreign counterintelligence."[20] For FISA orders, a Foreign Intelligence

---

The official name of the Fourteen Eyes is SIGNIT Seniors Europe, and its main purpose is to "coordinate the exchange of military signals amongst its members." *Id.*

16 For example, documents leaked by Edward Snowden show Australia's surveillance agency offered to share "bulk, unselected, unminimised metadata" as long as no data targeted an Australian national. Ewen MacAskill, James Ball, & Katharine Murphy, *Revealed: Australian Spy Agency Offered to Share Data About Ordinary Citizens*, GUARDIAN (Dec. 1, 2013), https://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens. Former United Kingdom home secretary, David Blunkett has said that "the NSA and . . . the U.S. use material gathered from network and service providers and offer it rather than having it sought from them in a way that makes authorization extremely difficult." This would mean that GSHQ circumvented domestic laws by obtaining information without seeking ministerial approval, reaching information unobtainable by legal means. Nicholas Watt, *NSA 'Offers Intelligence to British Counterparts to Skirt UK Law,'* GUARDIAN, June 10, 2013, https://www.theguardian.com/politics/2013/jun/10/nsa-offers-intelligence-british-counterparts-blunkett.

17 Wendy Everette, Comment, "*The FBI Has Not Been Here [Watch Very Closely for the Removal of This Sign]": Warrant Canaries and First Amendment Protection for Compelled Speech*, 23 GEO. MASON L. REV. 377, 378 (2016).

18 *Id.* at 383. Before Congress passed the USA Freedom Act, NSL recipients could not disclose the fact they had received an order to anyone but their attorney and the staff members that retrieved the requested information. *Id.*

19 *Foreign Intelligence Surveillance Act (FISA)*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/surveillance/fisa/ (last visited Oct. 17, 2016). FISA has been amended several times to include physical searches, pen registers, trace and trap devices, and increased presidential authority to approve limited physical searches without court orders. *See* James G. McAdams, III, *Foreign Intelligence Surveillance Act (FISA): An Overview*, FED. L. ENFORCEMENT TRAINING CTRS. 4 (2007), http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/researchby-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf.

20 MCADAMS, III, *supra* note 19, at 2. After the September 11 attacks, the USA Patriot Act changed the previous requirement that mandated *the only purpose* of the proposed surveillance was to obtain foreign intelligence and amended it so that the applicant only needed to certify that a significant purpose of the surveillance was to obtain foreign intelligence. *Id.* at 6.

Surveillance Court judge approves a request after reviewing the intended target and the presented accompanying procedures meant to minimize broad data collection. However, before the request is considered by the FISC judge, the U.S. Department of Justice (DOJ) reviews the agency's request prior to its submission.[21]

The DOJ's application must contain statements that show the targeted individual is a foreign power or an agent of a foreign power, certification from a high-ranking executive branch official detailing that the information to be obtained is foreign intelligence information that cannot be obtained by normal investigative techniques, include information about any previous applications surrounding the target, and list the type of communication or activities to be subject to the surveillance and contain a description of the information sought.[22] Upon approval, court orders can be used to survey targets, access metadata, and other content.[23]

It is critical to note that the only information available to the FISC is what is provided by the DOJ.[24] There is no opponent or adversarial balance to counter the DOJ's presentation.[25] Despite the fact that the court is reviewing information to certify the application meets statute's requirements, this is not enough oversight. The U.S. government's failure to respect individuals' privacy in crossing legal boundaries casts tremendous doubt on the FISC.[26] At the very least, the appearance of fairness is undermined by the Snowden revelations, and the lack of

21 *Foreign Intelligence Surveillance Act (FISA)*, *supra* note 19. Precisely, "[t]he Attorney General must personally approve each final FISA application." *Id.*

22 *Id.* The application must also present the proposed length of time, disclose if physical entry to the location is required, and present any minimization procedures regarding the acquisition, use, and retention of information "concerning nonconsenting U.S. persons." *Id.* "One common minimization procedure is what is known as an 'information-screening wall.' These 'walls' require an official not involved in the criminal investigation to review the raw materials gathered by FISA surveillance and only pass on information that might be relevant evidence."

23 Everette, *supra* note 17, at 392.

24 *Foreign Intelligence Surveillance Act (FISA)*, *supra* note 19. The FISC judge is completely reliant on the DOJ's representations in assessing whether the application has probable cause showing

> That one of four [following] conditions has been met: (1) the target knowingly engages in clandestine intelligence activities on behalf of a foreign power which 'may involve' a criminal law violation; (2) the target knowingly engages in other secret intelligence activities on behalf of a foreign power under the direction of an intelligence network and his activities involve or are about to involve criminal violations; (3) the target knowingly engages in sabotage or international terrorism or is preparing for such activities; or (4) the target knowingly aids or abets another who acts in one of the above ways.

Id. See also Everette, *supra* note 17, at 391.

25 Foreign Intelligence Surveillance Act (FISA), supra note 19.

26 See generally Glenn Greenwald, Fisa Court Oversight: A Look Inside a Secret and Empty process, GUARDIAN (June 18, 2013, 19:36 EDT), https://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy.

transparency as provided by FISA does little to assuage concerns that surveillance is being conducted as permitted by law.

In a post-Snowden world, knowing the extent of government surveillance and corporate compliance, intelligence sharing between nations threatens the privacy rights of citizens and its transnational neighbors. Distortion of the use of secret government surveillance, shrouded by secret intelligence-sharing agreements, threatens the public debate surrounding national security and individual privacy. This distortion persists on an international scale through the collaboration between national security agencies in the United States and their Five Eyes allies.

In 2017, several leaks plagued the Trump administration in its first year, cracking the foundation of trust among Five Eyes nations.[27] In May 2017, British officials condemned leaks [28] from the investigation surrounding the Manchester bombing, [29] and even temporarily paused the sharing of information with American law enforcement.[30] Earlier that month, President Trump was criticized for reportedly sharing sensitive information about Islamic State in Iraq and Syria (ISIS) operations by another U.S. ally, Israel, with Russia, against their wishes.[31] While the

---

27 Overton, supra note 11.

28 Ewen MacAskill & Julian Borger, Photographs of Manchester Bomb Parts Published After Leak, GUARDIAN (May 24, 2017), https://www.theguardian.com/uk-news/2017/may/24/us-officials-leak-more-manchester-details-hours-after-uk-rebuke. The New York Times published images of shrapnel, remnants of the bomb, and the backpack worn by the attacker on May 24, 2017, only two days after the attack. C.J. Chivers, Found at the Scene in Manchester: Shrapnel, a Backpack and a Battery, N.Y. TIMES (May 24, 2017), https://www.nytimes.com/interactive/2017/05/24/world/europe/manchester-arena-bomb-materials-photos.html. In addition, the attacker's name was also released by U.S. media while unreleased details concerning the bomber were disclosed by a French official.

29 On May 22, 2017, a bombing had occurred at a concert in Manchester, England that resulted in multiple deaths. Camila Domonoske, British Police Decry Apparent U.S. Leaks of Manchester Attack Evidence, NPR (May 25, 2017, 11:18 AM), https://www.npr.org/sections/thetwo-way/2017/05/25/530006788/british-police-decry-apparent-u-s-leaks-of-manchester-attack-evidence. As a part of international counterterrorism efforts, U.K. officials worked with international law enforcement groups to investigate the attack, including the United States. Id.

30 Jake Kanter, US Secretary of State Rex Tillerson 'Regrets' Manchester Bombing Leaks, BUS. INSIDER (May 26, 2017, 8:58 AM), http://www.businessinsider.com/rex-tillerson-regrets-manchester-bombing-leaks-2017-5. Commenting on the leaks surrounding the Manchester bombing investigation, President Trump called the situation "deeply troubling" and "a grave threat to… national security" before concluding that "[t]here is no relationship… cherish[ed] more than the Special Relationship between the United States and the United Kingdom." Statement from President Donald J. Trump, WHITE HOUSE (May 25, 2017), https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-6/.

31 Adam Goldman, Eric Schmitt & Peter Baker, Israel Said to Be Source of Secret Intelligence Trump Gave to Russians, N.Y. TIMES (May 16, 2017), https://www.nytimes.com/2017/05/16/world/middleeast/israel-trump-classified-intelligence-

President's actions did not receive any admonition from Israel,[32] the disclosure was seen as a "breach of espionage etiquette" that could discourage American allies from sharing helpful information with the United States.[33] Despite efforts to eliminate these leaks,[34] sensitive information continues to be impermissibly shared.[35] The impact of these

russia.html; Mark Hensch, Israeli Intelligence 'Boiling Mad' Over Trump Disclosure: Report, HILL (June 16, 2017), http://thehill.com/homenews/administration/333670-israeli-intelligence-boiling-mad-at-trump-report. Several news outlets identified Israeli intelligence as the source of the information. See Hensch, supra; Goldman et al, supra; Shane Harris, Israeli Source Seen as Key to Countering Islamic State Threat; WALL ST. J. (May 18, 2017, 4:16 PM), https://www.wsj.com/articles/israeli-source-seen-as-key-to-countering-islamic-state-threat-1495068912; see also Harris, supra (discussing potential harms to counterterrorism efforts, relationships with allies, and the intelligence community).

32 Joshua Mitnick, Former Top Israeli Officials Break With Government Line and Call Trump Leak Very Troubling, L.A. TIMES (May 17, 2017, 3:55 PM), http://www.latimes.com/world/middleeast/la-fg-israel-trump-russia-20170517-story.html. Peter Beaumont, Netanyahu and Trump Speak on Phone Amid Growing Row Over Russia Leak, GUARDIAN (May 17, 2017, 08:20 AM), https://www.theguardian.com/world/2017/may/17/netanyahu-trump-phonecall-israel-russia-intelligence-leak. Yisrael Katz, Israel's intelligence minister, commented on the matter, saying, "Intelligence cooperation between Israel and the United States regarding the threats posed by Iran and its proxies and Isis and its affiliates will continue and deepen." Id. However, other unnamed sources stated their frustration with the U.S. over the situation. See Kavitha Surana, Dan De Luce & Robbie Gramer, Israeli Intelligence Furious Over Trump's Loose Lips, FOREIGN POLICY (May 19, 2017, 3:32 PM), http://foreignpolicy.com/2017/05/19/israeli-intelligence-furious-over-trumps-loose-lips-russia-iran-syria/.

33 Peter Baker & Julie Hirschfeld Davis, Trump Defends Sharing Information on ISIS Threat with Russia, N.Y. TIMES (May 16, 2017), https://www.nytimes.com/2017/05/16/us/politics/trump-intelligence-russia-classified.html. See also Jack Moore, U.S. Officials 'Warned Israel' Not to Share Sensitive Intel With Trump, NEWSWEEK (May 16, 2017, 6:05 AM), http://www.newsweek.com/us-officials-warned-israel-not-share-sensitive-intel-trump-609782. This alleged breach violates "the most jealously guarded and sensitive areas of intelligence activity…which shields information supplied to an agency by intelligence partners in other countries from attribution." INTERNATIONAL INTELLIGENCE COOPERATION AND ACCOUNTABILITY, supra note 10, at 5.

34 Zeke J. Miller, The Trump Administration Pledges to Crack Down on Leaks, TIME (Aug. 5, 2017, 9:00 AM), http://time.com/4887864/trump-leaks-crackdown/. The leaks emerging from this administration have drawn attention to the inner workings of the Trump administration. See Callum Borchers, While Trump Tweets About 'Fake News,' His Leak Problem Is Worsening, WASH. POST (Oct. 5, 2017), https://www.washingtonpost.com/news/the-fix/wp/2017/10/05/while-trump-tweets-about-fake-news-his-leak-problem-is-worsening/?utm_term=.d7d3c4aa6620; Niall Stanage, Trump White House Besieged by Leaks, HILL (Feb. 9, 2017, 6:00 AM) http://thehill.com/homenews/administration/318621-trump-white-house-besieged-by-leaks. The continued leaks leave a "'corrosive effect' on global data sharing with Washington" and reflect an internal distrust amongst President Trump and the intelligence community; Yonah Jeremy Bob, Exclusive: Ex-US Intel Chief Says Trump Leaks Have A 'Corrosive' Effect, JERUSALEM POST (Aug 11., 2016, 11:09 AM), http://www.jpost.com/International/Ex-US-intel-chief-Trump-leaks-have-a-corrosive-effect-502125.

35 Jack Moore, Trump Team Leaks About Israel's Hack of Kaspersky Lab Could Further 'Damage' Ties, Experts Warn, NEWSWEEK (Oct. 17, 2017, 6:10 AM), http://www.newsweek.com/trump-team-leaks-about-israels-hack-kaspersky-lab-could-further-damage-ties-686500; Callum Paton, Trump White House's latest strategy to deal with leaks…has been leaked, NEWSWEEK (Aug. 14, 2017, 7:47 AM), http://www.newsweek.com/trump-white-houses-newest-strategy-deal-leaks-has-been-leaked-664756.

leaks will likely hamper the freer flow of information between these countries that developed after 9/11.[36]

The American reaction to 9/11 involved a shift in foreign policy, which included significant reforms in its intelligence community.[37] The years following the attack and the changes which followed have left an indelible mark on the global fight against terrorism.[38]

The United States and the international community soon recognized that the "old terrorism" of the Cold Era had dissipated, leaving a new sort of threat.[39] In response, Congress developed extensive legislation tackling national security, including international and domestic surveillance.[40] To assist in the fight against terrorism, Congress passed the USA Patriot Act ("Patriot Act") which emboldened the Department of Justice's investigation into 9/11.[41] The Patriot Act contained "the most sweeping

36 Overton, supra note 11.

37 BRENT DURBIN, THE CIA AND POLITICS OF US INTELLIGENCE REFORM 209-10 (2017). One of the primary factors attributed to allowing such an attack to occur in the United States was the poor coordination and information-sharing between federal agencies. Id. at 8; NATIONAL SECURITY, SURVEILLANCE, AND TERROR: CANADA AND AUSTRALIA IN COMPARATIVE PERSPECTIVE 52 (Randy K. Lippert, et al., eds. 2016) [hereinafter NATIONAL SECURITY, SURVEILLANCE, AND TERROR].

38 The fight against international terrorism resulted in greater amounts of information being shared among concerned nations and larger collaborative efforts in combatting global threats. INTERNATIONAL INTELLIGENCE COOPERATION AND ACCOUNTABILITY, supra note 10, at 2. Similarly, the scope of intelligence operations has also expanded to include both "non-traditional allies" and "a wider variety" of activities. Id. The events of September 11, 2001 led to a "radical restructuring" of American national security agencies and their activities. DURBIN, supra note 37, at 207.

39 NATIONAL SECURITY, SURVEILLANCE, AND TERROR, supra note 37, 51-52. During the Cold War era, "transnational terrorism was primarily motivated by a range of political ideologies associated with nationalism, separatism, Marxism and nihilism," but this threat was largely state-sponsored. Id. In contrast, the terrorist attacks of September 11, 2011 drew attention to a different type of terrorism that was "diffusely structured" and sponsored by non-state actors. Id. at 52. Still, the increased international cooperation seen today is primarily a result of globalization, and not of any particular event. INTERNATIONAL INTELLIGENCE COOPERATION AND ACCOUNTABILITY, supra note 10, at 11.

40 DURBIN, supra note 37, at 211. However, the resulting congressional action "lacked direction." William Crotty, On the Home Front: Institutional Mobilization to Fight the Threat of International Terrorism, in THE POLITICS OF TERROR: THE U.S. RESPONSE TO 9/11 191, 196 (William Crotty ed. 2016). See also id. at 196-97 (listing a series of congressional actions made in response to 9/11). This legislation also has been criticized for its negative impact on civil liberties. Tara Mythri Raghavan, In Fear of Cyberterrorism: An Analysis of the Congressional Response, 2003 U. ILL. J. L. TECH. & POL'Y 297, 311 (2003); John W. Whitehead & Steven H. Aden, Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA Patriot Act and the Justice Department's Anti-Terrorism Initiatives, 51 AM. U. L. REV. 1081, 1083 (2002). Despite this criticism, at the time of this legislative reform, constituent interests favored national defense over individual liberties due to the perceived external threat to the country's security and protection. DURBIN, supra note 37, at 266.

41 Id. at 1088. At the time of its passage, then Attorney General John Ashcroft commented that,

> Within hours of [its] passage…we made use of its provisions *to begin enhanced information sharing between the law-enforcement and intelligence communities.* We have used the provisions allowing nationwide search warrants for e-mail and subpoenas for payment information. And we have used the Act to place those who access the Internet through cable companies on the same footing as everyone else.

expansion of government surveillance authorities" in decades.[42] However, the extent of surveillance was not fully known until a few years later, with the 2013 controversy surrounding Edward Snowden.[43] The information disclosed about the United States' data collection and surveillance programs catalyzed a new focus on privacy concerns among scholars and the public.[44]

Id. (emphasis added).

42 DURBIN, *supra* note 37, at 214. The bill passed with overwhelming support, and although "privacy-minded lawmakers" were concerned with its expansive surveillance powers, not much was done to address these fears. *Id.* However, concerned legislators did manage to insert a sunset clause of four years for several provisions. *Id.* at 213. The Act included amendments to the Foreign Intelligence Surveillance Act (FISA), Electronic Communications Privacy Act (ECPA), and Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (more commonly known as the "Wiretap Act"). *USA Patriot Act*, EPIC.ORG, https://www.epic.org/privacy/terrorism/usapatriot/ (last visited Jan. 5, 2018). For instance, Section 216 of the Patriot Act extended the Wiretap Act to "authorize the installation of [such] devices to record all computer routing, addressing, and signaling information…by certifying that the information likely to be obtained is relevant to an ongoing criminal investigation." John Podesta, *USA Patriot Act: The Good, the Bad, and the Sunset*, HUMAN RTS., Winter 2002, at 1. The Act also allowed the transmission of intercepted "foreign intelligence information" to "any Federal Law enforcement, intelligence, protective, immigration, national defense, or national security official" when it facilitates the "performance of [the] official duties" of the individual receiving the information. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 445 (codified as amended at 50 U.S.C. §§ 3365) [hereinafter Patriot Act]. The Patriot Act also broadened the definition of terrorism to include "domestic" terrorism; *see How the USA Patriot Act Redefines "Domestic Terrorism,"* ACLU, https://www.aclu.org/other/how-usa-patriot-act-redefines-domestic-terrorism (last visited Jan. 5, 2018) (critiquing the expansion of the definition of terrorism to include domestic groups); Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended at 18 U.S.C. §§ 2331).

43 DURBIN, *supra* note 37, at 236. In 2013, former CIA employee and NSA contractor, Edward Snowden, revealed himself to be the source of a series of documents describing NSA programs and surveillance activities against U.S. and foreign citizens; Kim Zetter, *NSA Contractor Outs Himself as Source of Surveillance Documents*, WIRED (June 9, 2013), https://www.wired.com/2013/06/nsa-leaker-outs-himself/. Discussing his decision to release the documents Snowden stated that the NSA's surveillance practices are "an existential threat to democracy." Glenn Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. The Snowden documents also revealed foreign governments' surveillance activities as well; *see* Nick Hopkins, *UK Gathering Secret Intelligence Via Covert NSA Operation*, GUARDIAN (June 7, 2013), https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism ("UK security agency GCHQ gaining information from world's biggest internet firms through US-run Prism programme."); Philp Dorling, *Exposed: Australia's Asia Spy Network*, SYDNEY MORNING HERALD (Oct. 31, 2013), http://www.smh.com.au/federal-politics/political-news/exposed-australias-asia-spy-network-20131030-2whia.html ("A secret US National Security Agency document leaked by Mr Snowden … reveal[ed] the existence of a highly sensitive signals intelligence collection program conducted from sites at US embassies and consulates and from the diplomatic missions of other "Five eyes" intelligence partners including Australia, Britain and Canada.")

44 *See* Ashley Deeks, *An International Framework for Surveillance*, 55 VA. J. INT'L L. 291, 326 (2015). "The Snowden revelations initiated a large number of inter-state interactions and critical public statements about the legality and propriety of surveillance of foreign leaders and citizens." *Id.*; *see*

The Snowden disclosures uncovered a trove of information regarding the current intelligence-sharing practices of the United States and its foreign partners, including the remaining Five Eyes nations. The leak revealed that Britain's premier spy agency, the Government Communications Headquarters (GCHQ), had "secretly gained access to the network of cables which carry the world's phone calls and internet traffic" and could process large amounts of "sensitive personal information which it [shared] with its American partner, the National Security Agency."[45] Moreover, about 850,000 NSA employees and U.S. private contractors had access to GCHQ databases.[46]

The information-sharing between Five Eyes nations continues to advance as security threats develop. In 2017, the U.S. began working on cooperative cyber operations with its Five Eyes allies.[47] United States Cyber Command ("CYBERCOM"),[48] the unified combatant command[49] charged with "the planning and execution of global cyberspace

generally Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CENTER (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

45 Ewen MacAskill, *GCHQ Taps Fibre-Optic Cables For Secret Access to World's Communications*, GUARDIAN (Jun. 21, 2013, 12:23 PM), https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

46 *Id.*

47 Mark Pomerleau, *Coming Soon: Joint International Cyberspace Operations*, C4ISRNET (June 16, 2017). https://www.c4isrnet.com/disa/disa-vision-guide/2017/06/16/coming-soon-joint-international-cyberspace-operations/. A U.S. intelligence official shared that the cooperation could be "threat intelligence information where each nation is acting independently but synchronized….one nation supporting another with capability or capacity on another nation's host networks…[or] integrated operations on a shared environment." *Id.*

48 CYBERCOM is a unified combatant command first created in 2009 to respond to cyber-attacks. Jim Garamone & Lisa Ferdinando, *DOD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command*, U.S. DEP'T OF DEF. (Aug. 18, 2017), https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/. CYBERCOM "unifies the direction of cyberspace operations" within the U.S. Department of Defense and contains service elements from the Army, Navy, Air Force, Marines, and Coast Guard. *U.S. Cyber Command (USCYBERCOM)*, U.S. STRATEGIC COMMAND (Sept. 30, 2016), http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/.

49 A unified combatant command is a "command with broad continuing missions under a single commander…that is established and so designated by the President." JOINT CHIEFS OF STAFF, DOCTRINE FOR THE ARMED FORCES OF THE UNITED STATES xix (2013). Combatant Commands are given command authority over assigned forces to complete their proscribed mission as established by the President. *Id.* at xix, IV-5. CYBERCOM was elevated to a full unified combatant command by President Trump in August 2017. Mark Pomerleau, *DOD Still Working Toward CYBERCOM Elevation*, FIFTH DOMAIN (Oct. 16, 2017), https://www.fifthdomain.com/dod/cybercom/2017/10/16/dod-still-working-toward-cybercom-elevation/.

operations,"[50] first drafted its concept of operations draft[51] with the Five Eyes allies.[52] A top official at CYBERCOM explained that the inclusion of Five Eyes partners in this effort "truly acknowledge[d] the global nature of cyberspace and the benefit of collaboration to protect…infrastructure and defend against our mutual adversaries."[53] Collaborating with Five Eyes partners was a clear choice for CYBERCOM as "[w]hen it comes to the sharing of information with regards to defensive cyberspace operations, the mechanisms are already there."[54] As the U.S. expands its cyber operations, it will continue to rely on the "robust intelligence sharing" already in place, deepening the links within the Five Eyes alliance. [55] While the U.S. regularly collaborates with other nations in intelligence operations, Britain remains its closest partner in this endeavor.[56] In fact, the partnership between the U.S. and U.K. is so close that "it becomes very difficult to know who is doing what."[57]

B. The United Kingdom

The Snowden disclosures have prompted global dialogues over American governmental surveillance and have raised concerns about intelligence-sharing with and among its partners, particularly the United Kingdom.[58] According to documents leaked by Snowden in 2013, phone,

---

50 Mark Pomerleau, *Cyber Command Greater New, Expanded Authorities*, FIFTH DOMAIN (Feb. 28, 2018), https://www.fifthdomain.com/dod/cybercom/2018/02/28/cyber-command-granted-new-and-expanded-authorities/.

51 Concept of operations, also known as CONOPS, is "[a] verbal or graphic statement that clearly and concisely expresses what the commander intends to accomplish and how it will be down using available resources." JOINT CHIEFS OF STAFF, DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS 48 (2018).

52 Mark Pomerleau, *US Seeks Stronger International Cyber Defense Partnerships*, FIFTH DOMAIN (June 14, 2017), https://www.c4isrnet.com/disa/disa-vision-guide/2017/06/14/us-seeks-stronger-international-cyber-defense-partnerships/.

53 *Id.*

54 Pomerleau, *supra* note 47.

55 *Id.*

56 Yusra Aziz, *The Five Eyes Intelligence Alliance*, PRIVACY END (July 17, 2017), https://www.privacyend.com/five-eyes-intelligence-alliance/.

57 *Id.*

58 *See* Laura Poitras et al., *NSA Spied on European Union Offices*, DER SPIEGEL (Jun. 29, 2013), http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html; Lana Lam, *Edward Snowden: US Government Has Been Hacking Hong Kong and China for Years*, SOUTH CHINA MORNING POST (June 14, 2013), http://www.scmp.com/news/hong-kong/article/1259508/edward-snowden-us-g

overnment-has-been-hacking-hong-kong-and-china; Dan Roberts and Spencer Ackerman, *US Lawmakers Call for Review Of Patriot Act After NSA Surveillance Revelations*, GUARDIAN (Jun. 10, 2013), https://www.theguardian.com/world/2013/jun/10/patriot-act-nsa-surveillance-review.

internet, and email records of British citizens have been analyzed and stored by the NSA.[59] Moreover, this practice was approved by UK intelligence officials.[60] Other Five Eyes countries also participated in these activities, which included the capture of "incidentally collected" communications by the NSA, resulting in untargeted individuals' information being stored.[61] This means that individuals not suspected of any wrongdoing had their information collected by a foreign state, which then freely shared that information with their local government, circumventing any domestic safeguards in place.[62] The Snowden disclosures also revealed that in 2005, the NSA put forth a procedure about spying on British and other Five Eye nation citizens when the partner government has expressly forbidden the U.S. from doing so.[63] Additionally, in 2014 it was revealed that the GCHQ utilized a NSA database that the U.S. government has used to collect and store

59 James Ball, *US And UK Struck Secret Deal To Allow NSA To 'Unmask' Britons' Personal Data*, GUARDIAN (Nov. 20, 2013), https://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data.

60 *Id.*

61 *Id.* In addition, the NSA used British citizens' data to direct "pattern of life" analysis which allows the examination of parties related to a target by a friend of a friend of a friend. For a typical Facebook user, this could extend to more than 5 million people. *Id.*

62 Public authorities in the United Kingdom like the "Government Communication Headquarters (GCHQ) can also serve secret legal processes with non-disclosure orders similar to those mentioned above under the Regulation of Investigatory Powers Act (RIPA)." Jon Penney, *Warrant Canaries Beyond the First Amendment: A Comment*, *in* INTERNET MONITOR 2014: REFLECTIONS ON THE DIGITAL WORLD 49, 49 (Harvard Univ. Berkman Klein Center for Internet & Society ed. 2014). Additionally, law enforcement officials in the UK are able to force technology companies to hand over encryption keys. The law also makes it a criminal offense for the affected company to provide notice to users that an encryption key has been provided. Alessandro Liotta, *New Powers to Compel Decryption and Disclosure of Encryption Keys*, INT'L L. OFFICE (Nov. 20, 2007), http://www.internationallawoffice.com/Newsletters/IT-Internet/United-Kingdom/Pillsbury-Winthrop-Shaw-Pittman-LLP/New-Powers-to-Compel-Decryption-and-Disclosure-of-Encryption-Keys. Legally requiring these organizations to produce these keys is another form of compelled speech. Penney, *supra* note 62, at 50. This type of compelled speech has been of particular concern in the U.S. recently due to Apple's dispute with the FBI over decrypting a suspect's iPhone which raised key Fifth Amendment concerns. David Kravets, *Forget the 1st Amendment, Apple to Plead the 5th in Iphone Crypto Flap*, ARS TECHNICA (FEB. 24, 2016, 3:32 PM) http://arstechnica.com/tech-policy/2016/02/forget-the-1st-amendment-apple-to-plead-the-5th-in-iphone-crypto-flap/. In the United Kingdom, some technologies companies have chosen to provide an explanation every time they revoke a key voluntarily, but when forced by authorities to revoke encryption keys an explanation is not provided. This practice is known as "tipping off" others that a law enforcement request prompted the encryption key's revocation. Penney, *supra* note 62, at 51. No clear legal basis currently exists to protect this practice though. *Id.* For example, "[t]he UK Human Rights Act (1998) includes rights to freedom of expression under Article 10, but this right is explicitly 'qualified' and can be limited for a host of state objectives, including 'national security,' 'territorial integrity,' 'public safety, [sic] and 'prevention of disorder . . .'" *See id.*

63 Penney, *supra* note 62, at 51. The memo also specified that partner countries cannot be informed of the surveillance or the procedures used. *Id.*

approximately 200 million global text messages daily to search for information on individuals in the U.K.[64]

A greater source of concern in the U.K. is the recent passage of legislation, the Investigatory Powers Act 2016 ("IPA"), granting the British government sweeping surveillance powers. This legislation enables the British government to keep a record of every website each citizen visits for up to a year.[65] This law is also in conflict with the General Data Protection Regulation (GDPR) which was approved by the European Union Parliament.[66] In response to its passage, over 200,000 people signed a petition asking for the IPA's repeal.[67] Liberty, a civil liberties group, successfully crowdfunded over £50,000 to challenge the Act's expansive grant of surveillance powers to the British government.[68] In June 2017, the British High Court granted the organization permission to continue their challenge against the UK government.[69] An added complication is the effect of the United Kingdom's referendum to leave the European Union in June 2016.[70] However, the United Kingdom is not set to leave the EU

64 *Edward Snowden: Leaks That Exposed US Spy Programme*, BBC NEWS (Jan. 17, 2014), http://www.bbc.com/news/world-us-canada-23123964.

65 James Vincent, *The UK Now Wields Unprecedented Surveillance Powers- Here's What It Means*, VERGE (Nov. 29, 2016, 12:05 PM), http://www.theverge.com/2016/11/23/13718768/uk-surveillance-laws-explained-investigatory-powers-bill. This information would include what times an individual visited a site, the IP address used, and information about the computer used to access the domain. *Id.*

66 Pascal Crowe, *Could the European GDPR Undermine the UK Investigatory Powers Act?*, LONDON SCHOOL OF ECONOMICS & POLITICAL SCIENCE: MEDIA POLICY PROJECT BLOG (Dec. 19, 2016), http://blogs.lse.ac.uk/mediapolicyproject/2016/12/19/could-the-european-gdpr-undermine-the-uk-investigatory-powers-act/.

67 Claire Hopping, *Liberty Launches Legal Challenge Investigatory Powers Act*, ITPRO (Mar. 2, 2017), http://www.itpro.co.uk/it-legislation/28251/liberty-launches-legal-challenge-against-investigatory-powers-act.

68 Rene Millman, *Liberty Wins Right to Challenge Snoopers' Charter*, ITPRO (June 30, 2017), http://www.itpro.co.uk/it-legislation/28973/liberty-wins-right-to-challenge-snooper-s-charter; *see also The People vs The Snoopers' Charter*, LIBERTY HUM. RTS, https://www.liberty-human-rights.org.uk/campaigning/people-vs-snoopers-charter (last visited May 7, 2018).

69 Millman, *supra* note 68. Liberty was granted permission to attack the IPA provision that forces Internet Service Providers ("ISPs") to retain logs of everyone's "emails, phone calls, texts and entire web browsing history" to turn over to state agencies. *Id.* Liberty also was granted permission to challenge several other provisions of the IPA, beginning March 2018 at the latest. *Id.* Liberty also looks to attack the IPA's grant of three other bulk powers: bulk interception (the British government's collection and surveillance of calls without "any suspicion of criminal activity"), bulk hacking (the government's ability to "access, control, and alter electronic devices"), and bulk personal data sets (the government's ability to control and connect private and public databases containing a swath of information "ripe for abuse and discrimination"). Natasha Lomas, *Liberty is Crowdfunding a Legal Challenge to UK Surveillance Law*, TECHCRUNCH (Jan. 9, 2017), https://techcrunch.com/2017/01/09/liberty-is-crowdfunding-a-legal-challenge-to-uk-surveillance-law/.

70 Alex Hunt and Brian Wheeler, *Brexit: All you need to know about the UK leaving the EU*, BBC (Jan. 24, 2017), http://www.bbc.com/news/uk-politics-32810887.

until Summer 2019, prior to when the GDPR must be implemented by the UK as a EU Member State.[71] The provisions of the GDPR provide strong incentives for compliance, since data controllers found in breach can face fines up to 4%[72] of global annual gross revenue or €20 million.[73]

In March 2015, Privacy International, a United Kingdom-based nongovernmental organization (NGO) focused on championing privacy rights, along with nine other NGOs, filed an application to the European Court of Human Rights (ECHR) challenging the British government's surveillance practices.[74] The application specifically contests the bulk interception of Internet traffic in the United Kingdom's fiber-optic cables and the British government's access to information shared by the United States from their intelligence-gathering procedures.[75] The Application complains that the British government "asserts an almost unfettered right to obtain those [communications] which have been intercepted by the intelligence services of other states, including the National Security Agency (NSA) of the United States of America." [76] The application is the result of several legal complaints brought before the United Kingdom Investigatory Powers Tribunal and were joined together.[77] The Tribunal

71 Liat Clark, *What Theresa May's Brexit Plans Could Mean for You, Your Data, and Your Privacy*, WIRED (Oct. 24, 2016), http://www.wired.co.uk/article/the-uk-needs-europes-data-protection-laws.

72 Hasan, *supra* note 71; Jonathan Millard & Tyler Newby, *EU's General Data Protection Regulation: Sweeping Changes Coming to European and U.S. Companies*, ABA PRIVACY & DATA SECURITY (May 23, 2016), http://apps.americanbar.org/litigation/committees/technology/articles/spring2016-0516-eu-general-data-protection-regulation.html.

73 That amount is equal to approximately 21,456,700.00 U.S. dollars. Previously, fines were capped at €1 million or 2% of the global gross revenue. European Commission Press Release IP / 15 / 5176, Commission Proposal on New Data Protection Rules to Boost EU Digital Single Market Supported by Justice Ministers, THE COMMISSION (June 15, 2015), http://europa.eu/rapid/press-release_IP-15-5176_en.htm.

74 The other nine NGOs participating are the American Civil Liberties Union, Amnesty International, Bytes for All, the Canadian Civil Liberties Union, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties, the Legal Resources Centre, and Liberty. Applicants' Reply to Observations of the Government of the United Kingdom at 35, App. No. 24960/15, *10 Human Rights Organisations v. The United Kingdom* [2014] (Eng.) [hereinafter *10 Human Rights Organisations Applicant Reply*].

75 *10 Human Rights Organisations v. United Kingdom*, PRIVACY INTERNATIONAL https://www.privacyinternational.org/node/992 [hereinafter *10 Human Rights Organisations*].

76 *10 Human Rights Organisations Applicant Reply*, *supra* note 74.

77 *UK NGOs Challenge UK Government Surveillance at the European Court of Human Rights*, OPEN RTS. GRP. (Nov. 7, 2017), https://www.openrightsgroup.org/press/releases/2017/uk-ngos-challenge-uk-government-surveillance-at-the-european-court-of-human-rights. In response to the Snowden revelations that repealed mass surveillance by UK intelligence agencies, Big Brother Watch, a UK-based civil liberties group, filed an application with the European Court of Human Rights. *Id.*; *About*, BIG BROTHER WATCH, https://bigbrotherwatch.org.uk/about/. Their application "challeng[ed] the legality of the indiscriminate surveillance of UK citizens and the bulk collection of vast amounts of

ruled that the British government's interception of information and any access to information supplied by the United States "[was] lawful in principle."[78] The application brought by the NGOs challenges the Tribunal findings.[79] In November 2017, the European Court of Human Rights heard arguments from both parties, and a decision is pending.[80]

The application relies on the Snowden disclosures regarding the United States intelligence-gathering programs and the Five Eyes Agreement to claim that United Kingdom Intelligence Services "are likely to have broad access to the fruits of US communications surveillance, including pursuant to the bulk surveillance programmes."[81] The existence of Five Eyes is a key premise to this concern since it establishes a "long-standing arrangement"[82] of intelligence-sharing between the United States and United Kingdom, culminating in British intelligence having access to hundreds of millions of text messages.[83]

---

their personal information and communications by UK intelligence agencies (including GCHQ) under the . . . Regulation of Investigatory Powers Act (RIPA) 2000" in violation of British citizens' right to a private life. *Big Brother Watch and Others v UK at the European Court of Human Rights*, BIG BROTHER WATCH (Nov. 3, 2017), https://bigbrotherwatch.org.uk/2017/11/big-brother-watch-and-others-v-uk-at-the-european-court-of-human-rights/. Additionally, the case questions "whether greater controls are needed on the receipt of intercepted foreign intelligence so that it doesn't circumvent UK safeguards." *Id.*

78 *10 Human Rights Organisations*, *supra* note 75. The United Kingdom Investigatory Powers Tribunal ruled that in regards to the intelligence-sharing practices between the United States and United Kingdom the "rules need [not] [] be contained in statute [] or even in a code… Appropriate rules or *arrangements* exist and are publicly known and confirmed to exist, with their content sufficiently signposted, such as to give an *adequate indication* of it" and that these practices are indeed "subject to proper oversight." Liberty & Others vs. the Security Service, SIS, GCHQ [2014] UKIPTrib 13_77-H, 23, http://www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

79 *10 Human Rights Organisations*, *supra* note 75. In February 2015, the Tribunal found that information gathered prior to the proceedings was unlawful since the legal framework surrounding its collection was secret. *Id.* In June 2015, the Tribunal ruled that the British government illegally surveilled on two of the claimants, Amnesty International and the Legal Resources Centre. *Id.*

80 *Recap: 10 Human Rights Organisations vs. the United Kingdom*, PRIVACY INT'L (Nov. 7, 2017), https://www.privacyinternational.org/node/624.

81 *10 Human Rights Organisations Applicant Reply*, *supra* note 74, at 34. The Application mentions PRISM and Upstream along with the corresponding American legal authority, establishing what large amounts of information would be available through information-sharing agreements. *Id.* at 32.

82 *Id.* at 33-34. "Intelligence sharing between the US and UK must be viewed within the context of a long-standing arrangement between the intelligence activities of the two countries, along with Australia, Canada and New Zealand[.]" *Id.* at 33.

83 *10 Human Rights Organisations*, *supra* note 75. James Ball, *NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep*, GUARDIAN (Jan. 16, 2014), https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep. The claimants' complaint alleges the data interception and information-sharing violate Articles 8 and 10 of the European Convention on Human Rights; it also argues that the nation's bulk interception program discriminates based on national origin which violates Article 14. *10*

Britain's eventual exit from the European Union will have a complicated effect on its current data protection regime and its future data transfers with its former Member states.[84] The extent of the effect of Britain's exit from the EU upon its data protection regime and accompanying business interests is a question that can only be answered by watching what the United Kingdom will do in the coming years.[85] Until then, it is likely that the status quo regarding its intelligence-sharing practices with the U.S. and other Five Eyes countries will continue.[86]

C. Germany

After the Snowden leaks revealed that U.S. intelligence agencies had been monitoring Chancellor Angela Merkel and millions of other German citizens, the relationship between Germany and the United States became strained.[87] Germany asked the U.S. to form a "no spy" agreement, like other agreements allegedly already in existence between the U.S. and allies providing for intelligence-sharing between them.[88] The "no spy"

Human Rights Organisations, *supra* note 75; 10 *Human Rights Organisations Applicant Reply*, *supra* note 74, at 101-06. The application also alleges Article 6 violations in the Investigatory Powers Tribunal proceedings. *10 Human Rights Organisations v. UK*, ELEC. PRIVACY INFO. CTR., https://epic.org/amicus/echr/liberty-gchq/ (last visited Jan. 12, 2017).

84 Some Brexit supporters oppose the numerous regulations imposed and required by the European Union since it eradicates national sovereignty and stifles free markets. Presumably, the numerous data protections required by EU legislation and the European Court of Justice are viewed just as unfavorably. *How and why Brexit Triumphed*, ECONOMIST (Jan. 7, 2017), http://www.economist.com/news/books-and-arts/21713821-first-books-try-explain-shock-referendum-last-june-how-and-why-brexit. While the GDPR will apply to companies outside of the EU like the EU Data Protection Directive before it, if Britain chooses to be part of the European Economic Area (EEA), then the GDPR would apply directly to the United Kingdom. EUROPEAN COMM'N, TRANSFERRING YOUR DATA OUTSIDE OF THE EU (Mar. 12, 2015), http://ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm.

85 For example, in reference to Brexit, a Microsoft's UK Government Affairs Manager said that the company would reconsider its commitment to the UK as a result of its departure from the EU; Microsoft later clarified that this particular position expressed by a Microsoft employee was not "reflective of the company's views."" Peter Bright, *Microsoft Mulls Cutting UK Datacenter Investment Amid Brexit Concerns*, ARSTECHNICA (Jan. 23, 2017), https://arstechnica.com/information-technology/2017/01/brexit-tariff-fears-could-see-microsoft-cut-uk-datacenter-investment/?comments=1&post=32690447&mode=quote.

86 The other Five Eyes countries similarly impose nondisclosure orders and do not allow free speech or freedom of expression to overwhelm national security concerns. *See generally* Penney, *supra* note 62.

87 Anthony Faiola, *Germans, Still Outraged by NSA Spying, Learn Their Country May Have Helped*, WASH. POST (May 1, 2015), https://www.washingtonpost.com/world/europe/nsa-scandal-rekindles-in-germany-with-an-ironic-twist/2015/04/30/030ec9e0-ee7e-11e4-8050-839e9234b303_story.html?utm_term=.51ea5ce08fd3.

88 The referenced, pre-existing intelligence-sharing agreement, the UKUSA Agreement discussed in PART II, has been a matter of public record since 2010 after the declassification of a 1955 U.S.

agreement advocated by top German officials between the two countries never materialized.[89] Although the talks between Germany and the United States did not result in any formal agreements, President Obama pledged that the U.S. had "taken the unprecedented step of ordering our intelligence communities to take the privacy interests of non-U.S. persons into account in everything that they do—something that has not been done before and most other countries in the world do not do . . . ." President Obama further commented that the Unites States is "committed to a U.S.-

National Security Agency (NSA) document entitled "U.K.-U.S. Communications Intelligence Agreement." Kristina Daugirdas & Julian Davis Mortensen, *In Wake of Espionage Revelations, United States Declines to Reach Comprehensive Intelligence Agreement with Germany*, 108 AM. J. INT'L L. 815, 816 (2014). The current agreement between these countries is known as the "Five Eyes" agreement. The term "Five Eyes" refers to the governments of Australia, Canada, New Zealand, United Kingdom, and the United States. The term originates from the introduction of a new classification level, "SECRET – AUS/CAN/NZ/UK/US EYES ONLY," introduced by the intelligence-sharing agreement. James Cox, *Canada and the Five Eyes Intelligence Community*, OPENCANADA.ORG, https://www.opencanada.org/features/canada-and-the-five-eyes-intelligence-community/ (last visited Oct. 17, 2016).The document revealed "intelligence sharing between the United States, the United Kingdom, Australia, Canada, and New Zealand, includ[ing] provisions governing collection of signal traffic; acquisition of communications documents and equipment;…cryptanalysis; decryption and translation; and acquisition of information regarding communications organizations, procedures, practices, and equipment." Daugirdas & Mortensen, *supra*, at 816. The NSA's accompanying statement emphasized "[t]he bonds, forged in the heat of a world war and tempered by decades of trust and teamwork, remain essential to future intelligence successes." *Id.* In addition to public concern of American surveillance in Germany stemming from press coverage of the Snowden leaks, several German federal employees were arrested and suspected of sharing German intelligence with U.S. intelligence agencies which led to the departure of the Central Intelligence Agency's Berlin station chief. Joseph Fitsanakis, *German Court Sentences Intelligence Officer Who Spied for CIA*, INTELNEWS.ORG (Mar. 17, 2016), https://intelnews.org/2016/03/17/01-1873/.

89 According to a U.S. administrative official familiar with the negotiations, "'What the Germans want, and wanted, is that we would never do anything against their laws on their territory.' That is an agreement the United States 'has with no country.'" David E. Sanger, *U.S. and Germany Fail to Reach Deal on Spying*, N.Y. TIMES, May 2, 2014, at A3. The failure of both sides to reach a deal in the ensuing aftermath reportedly left German and U.S. officials angry, with each side blaming the other for the conflict. *Id.* President Obama commented on the matter, "It's not actually correct to say that we have a 'no-spy agreement' with Great Britain. That's not actually what happens. There's no country where we have a no-spy agreement. We have, like every other country, an intelligence capability, and then we have a range of partnerships with all kinds of countries." Daugirdas & Mortensen, *supra* note 88, at 818. During negotiations between President Obama's national security adviser, Susan E. Rice, and Chancellor Merkel's advisor of foreign policy, Christoph Heugsen, Ms. Rice allegedly revealed that the "United States did not have no-spy agreements with any of its close allies, even with the other members of the so-called Five Eyes . . . which share virtually all of their intelligence." Sanger, *supra* at A3. Ms. Rice also reportedly shared that "[a]ny such agreement with Germany would set a precedent that every other major European ally, along with the Japanese, the South Koreans and others, would soon demand to replicate." *Id. See also Federal Chancellery*, AMERICAN INST. FOR CONTEMPORARY GERMAN STUDIES, http://www.aicgs.org/issue/federal-chancellery/ (last visited Oct. 17, 2016). These statements suggest that while the United States is comfortable with deeper cooperation with its longstanding Western allies, the American government is hesitant to share the extent of its surveillance programs with some of its newer partners. *Id.*

German cyber dialogue to close further the gaps that may exist . . . to make sure that there is transparency and clarity about . . . our goals and our intentions[.]"[90] Although it appears no formal agreement, at least publicly, has been arranged between the United States and Germany, the NSA and the German BND have resumed joint surveillance since early 2016.[91]

Recent scandals have plagued the BND, such as recent revelations that the NSA's collection and surveillance of Germans' data was not completely unknown by German intelligence. Even more troubling are the reports that German intelligence knew the NSA was spying on German citizens in violation of domestic law.[92] The culmination of growing concerns over data protection, the BND, and Germany's relationship with the U.S. in the intelligence context exists in a newly proposed legislation amending Germany's legal framework surrounding government surveillance. Notably, the amendments proposed would permit Germany to monitor foreigners' communications, a practice that is currently illegal under the current G10 Act.[93] Like the U.S. legal guidelines regarding NSLs and FISA orders, the proposed BND bill lacks judicial oversight. Both the Federal Constitutional Court of Germany and the ECHR have determined that surveillance legislation missing independent supervision cannot stand by holding that "prior control by an independent body, such as . . . a judicial arrangement, is required when intrusive surveillance measures are likely to reveal highly personal information" and that "the omission of a requirement that an authorizing judge independently assess the reasonableness of suspicion [helped] violate an applicant's privacy

90 Daugirdas & Mortensen, *supra* note 88 at, 818-19.

91 Tina Bellon, *German Spies Revive Internet Snooping Work With U.S.: Reports*, REUTERS (Jan 3, 2016), http://www.reuters.com/article/us-germany-spying-usa-idUSKBN0UM29Z20160108.

92 *See generally* Malk Baumgärtner, Nikolaus Blome et al., *German Intelligence Under Fire for NSA Cooperation*, DER SPEIGEL (Apr. 24, 2015), http://www.spiegel.de/international/germany/german-intelligence-agency-bnd-under-fire-for-nsa-cooperation-a-1030593.html. As a result, De-Cix, "the world's largest Internet exchange point," is suing BND for legal orders issued to them requiring the mass surveillance of "communications flowing through its Frankfurt Internet exchange point" under German's G10 Act. David Meyer, *World's Biggest Internet Hub Sues German Government Over Surveillance*, FORTUNE (Sept. 16, 2016), http://fortune.com/2016/09/16/de-cix-surveillance-germany/. The G10 Act "is analogous to the controversial U.S. Foreign Intelligence Surveillance Act (FISA), and allows the strategic monitoring of international communications that flow through Germany." *Id*.

93Christine Gavalga, *German Foreign Intelligence Bill Fails Human Rights Standards*, CTR. FOR DEMOCRACY & PRIVACY (Aug. 24, 2016), https://cdt.org/blog/german-foreign-intelligence-bill-fails-human-rights-standards/. The bill creates three different types of protection for communications that is contingent on individual's nationality. *Id.* German nationals cannot have their information intentionally obtained by the BNS within German's borders nor can the BND compel a German communication service to do so. *Id.* EU citizens that are not German may have their information collected at any time if it is deemed necessary. The remaining class, non-EU foreigners, can have their information collected as necessary to combat domestic or foreign security risks at "an early stage." *Id.*

rights" respectively.[94]

Despite the tension supplied by the Snowden disclosures, German and American intelligence agencies are working together again due to renewed national security concerns after the Paris terrorist attacks.[95] Despite allegations that the United States had continued to attempt its use of the BND's technology to analyze European data, the German government has continued to work towards deeper cooperation with other countries to create a joint intelligence database.[96]

While the U.S. and its allies have worked together to form an international coalition to combat threats to their own national security, the international community has been sluggish in addressing threats to individual privacy rights.[97] There are substantial and compelling reasons for states' unwillingness to develop an international framework that regulates government surveillance, espionage, and data sharing. One of the most significant domestic and international concerns is the prevention of terrorism and national security.[98] The very nature of espionage itself requires secrecy to be effective as ongoing investigations and data collection are dependent on the other party remaining unaware of surveilling parties.

III. DEMOCRATIC GOVERNANCE THROUGH LITIGATION & THE PRIVACY SHIELD

While the ECHR has yet to rule *in 10 Human Rights Organisations v*

94 *Id.*

95 *See Germany Restarts Joint Intelligence Surveillance With US*, DEUTSCHE WELLE (Sept. 1, 2016), http://www.dw.com/en/germany-restarts-joint-intelligence-surveillance-with-us/a-18968519.

96 Sumi Somaskanda, *Is Big Brother coming to Germany?*, AL JAZEERA (Dec. 14, 2014), http://www.aljazeera.com/indepth/features/2016/12/big-brother-coming-germany-161213062129779.html.

97 Deeks, *supra* note 44, at 313-15. For example, the right to privacy has already been recognized by international bodies such as the United Nations and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibits unlawful interference with that right. Rikke Frank Joergensen, *Can Human Rights Law Bend Mass Surveillance?*, DANISH INST. FOR HUM. RTS. (Feb. 27, 2014), https://policyreview.info/articles/analysis/can-human-rights-law-bend-mass-surveillance.

Unlawful interference undisputedly applies to the collection of electronic communication or data of an individual. *Id.* Furthermore, the ICCPR requires states to affirmatively ensure they have a legal framework that actually protects privacy rights from such interference, regardless of its source. *Id.* However, there is no consensus regarding the applicable standards that demonstrate when government surveillance is unlawful. Deeks, *supra* note 44, at 305. States also disagree on the scope of this "right to privacy" and whether it applies extraterritorially. *Id*. So, while the ICCPR would allow a nation to raise an interstate complaint against an offending country, this complaint procedure is very unlikely to ever be used. Joergensen, *supra*.

98 Deeks, *supra* note 44, at 313-15.

United Kingdom, there have been significant developments regarding government surveillance and data transfers between the United States and United Kingdom under the Privacy Shield,[99] which is a result of the European Data Protection Directive .[100]

The EU Data Protection Directive prohibits data transfer from Member States to nations which do not have "adequate" levels of protection.[101] Since the United States was not one of the states deemed to have the requisite adequacy required under the Directive, the U.S. Department of Commerce and the European Commission underwent negotiations that resulted in the Safe Harbor Agreement.[102] The U.S. Department of Commerce proposed a "safe harbor" system designed to shelter data transfers from Article 25 of the EU Data Protection Directive, which proscribes data transfers to states without adequate levels of data protection.[103] The Safe Harbor Agreement integrated aspects of the EU Data Protection Directive and distilled them to seven key principles which U.S. companies had to comply with in order to fall under the agreement.[104] Critically, however, the European Commission determined Safe Harbor principles could be limited as necessary for national security, public interest, or law enforcement requests.[105] However, the Snowden disclosures regarding information-sharing between U.S. national intelligence agencies and private corporations led to the removal of Safe

99 *Privacy Shield Overview*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/Program-Overview (last visited Jan. 8, 2018). The EU Data Protection Directive called for national data protection agencies to be formed in each member state. Organizations need to register their databases with these national agencies and in certain cases gain prior approval before they can begin data processing. MARTIN A. WEISS & KRISTIN ARCHICK, CONGR. RESEARCH SERV., RL44257, U.S.-E.U. DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 3 (2016).

100 Interestingly, the EU Data Protection Directive was enacted because of growing concerns over data transfer bans between member states with stricter data protection standards and those member states with lesser levels of protection. Tracie B. Loring, Comment, *An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States*, 37 TEXAS INT'L L. J. 421, 431 (2002). While other legislation and regulations have further developed the legal framework of data protection in the European Union, the Data Protection Directive remains the most critical and comprehensive component in understanding data protection in Europe. Weiss & Archick, *supra* note 99.

101 Loring, *supra* note 100, at 435-36.

102 *Id.* at 451-52.

103 *Id*.

104 Weiss & Archick, *supra* note 99, at 5. Those seven data protection principles concerned notice, choice, onward transfer, security, data integrity, access, and enforcement. *See id.* at 5-6. Additionally, companies were not forced to comply with Safe Harbor nor its replacement, the Privacy Shield, as several statutory exemptions exist which allow U.S. companies alternatives in conducting data transfers outside of Europe. *See id.* at 7, 14.

105 *Id.* at 5.

Harbor.[106]

This decision was later criticized and struck down by the European Court of Justice in *Maximillian Schrems v. Irish Data Protection Commissioner*.[107] Maximillian Schrems filed a complaint with the Irish Data Protection Commissioner looking to enjoin Facebook's Irish subsidiary from transferring his personal data to their servers in the United States, troubled by government surveillance programs revealed by Edward Snowden.[108] Schrems objected to the 2000 European Commission ruling that the Safe Harbor provided an adequate level of protection.[109] Since the Irish data protection agency (DPA) dismissed the complaint as bound by the Data Protection Directive and the Commission's previous ruling on the Safe Harbor agreement, Schrems brought an action to the Irish High Court which asked the European Court of Justice to review the issue.[110] The European Court of Justice reviewed whether national "supervisory authorities could independently investigate challenges to the adequacy of protections provided by third states" through the Safe Harbor agreement.[111]

The court's ruling had a significant impact. The court determined that national data protection agencies did have the authority to investigate claims and organizations' compliance with the EU Data Protection Directive and the Charter of Fundamental Rights despite the Safe Harbor agreement by the European Commission.[112] Upon directly examining the Safe Harbor agreement, the European Court of Justice found it did not ensure the requisite level of data protection as required by the EU Data Protection Directive.[113] Article 25 of the Data Protection Directive

---

106 W. Gregory Voss, *The Future of Transatlantic Data Flows: Privacy Shield or Bust?*, 19 J. INTERNET L. 1, 10 (2016).

107 Kristina Daugridas & Julian Davis Mortensen, *European Union and United States Conclude Agreement to Regulate Transatlantic Personal Data Transfers*, 110 AM. J. OF INT'L L. 360, 362-63 (2016) [hereinafter *Personal Data Transfers*].

108 *Id.* at 362. The Irish subsidiary also operates as the European headquarters for Facebook. *Id*.

109 *Id.*

110 *Id.*

> The Irish DPA dismissed the complaint, finding that it had no basis to evaluate the complaint since Facebook adhered to the Safe Harbor Agreement and the Irish DPA was thus bound by the 2000 decision by the European Commission recognizing that Safe Harbor provided an 'adequate level of protection' as required by the [European Data Protection Directive].

Weiss & Archick, *supra* note 99, at 6.

111 *Personal Data Transfers*, *supra* note 107, at 362. *See also* Weiss & Archick, *supra* note 99, at 6-7.

112 Weiss & Archick, *supra* note 99, at 7. The national data protection agencies "'must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him.'" *Id.*

113 *Id.*

requires the European Commission to examine the domestic laws of a non-member state when ascertaining the adequacy of its data protection.[114] As a result, the European Commission's decision regarding Safe Harbor in 2000 was invalid, and *Schrems* eliminated the legal viability of Safe Harbor as a mechanism to allow data transfers to continue between the United States and Europe.[115] In reaching this decision, the European Court of Justice found that American "national security, public interest, and law enforcement" trumped the Safe Harbor principles when in conflict.[116] Safe Harbor allowed and even "enable[d]" American law enforcement's interference with European citizens' fundamental data rights.[117]

Prior to the *Schrems* ruling, the United States and the European Union were looking to change the legal framework of Safe Harbor.[118] A few months after the court's ruling, the United States and the EU announced a new agreement, the Privacy Shield, to replace Safe Harbor.[119] It is unclear if the Privacy Shield can survive future scrutiny or legal battles.[120] One of the more imminent challenges the Privacy Shield faces is the General Data Protection Regulation (GDPR); the Privacy Shield will need to be revised in order to conform with the new legal framework.[121] Max Schrems

114 *Id.*

115 *Id.*

116 *Id.*

117 *Id.*

118 *Personal Data Transfers*, *supra* note 107, at 362.

119 *Id.* at 365. The Privacy Shield is the current legal framework governing data transfers and processing between the United States and Member states of the European Union. Although it is similar to its predecessor, the Privacy Shield is stricter in certain areas. Doron S. Goldstein et al., *Understanding the EU-US "Privacy Shield" Data Transfer Framework*, 20 J. OF INTERNET L. 1, 18 (2016).

120 *Id.* at 21. European Parliament member, Jan Philipp Albrecht, called the Privacy Shield "'little more than a reheated serving of the pre-existing Safe Harbor decision' and a 'sellout of the fundamental EU right to data protection.'" Natasha Lomas, *Europe And US Seal 'Privacy Shield' Data Transfer Deal To Replace Safe Harbo*r, TECHCRUNCH (Feb. 2, 2016), https://techcrunch.com/2016/02/02/europe-and-us-seal-privacy-shield-data-transfer-deal-to-replace-safe-harbor/ [hereinafter Lomas, *Privacy Shield*]. In discussing the Privacy Shield's ability to withstand further scrutiny, Schrems said, "[I]t's not really a problem to challenge it" because "[t]here are so many options to kill it." Aaron Souppouris, *The EU-US Privacy Shield is Up, But Its Future Is In Doubt*, ENGADGET (Jul. 12, 2016), https://www.engadget.com/2016/07/12/eu-us-privacy-shield-data-protection/. *See also generally* Tomaso Falchetta, *New "Shield," Old Problems*, MEDIUM (July 8, 2016), https://medium.com/privacy-international/new-shield-old-problems-c23c646f681c#.mfc796i0z. Despite this uncertainty, more than fourteen hundred companies have signed up for the Privacy Shield including Facebook, Google, Twitter, and Amazon. *See Privacy Shield List*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/list (last visited Jan. 16, 2017). *See also* Natasha Lomas, *EU-US Privacy Shield Data Transfer Deal Faces Legal Challenge*, TECHCRUNCH (Oct. 27, 2016), https://techcrunch.com/2016/10/27/eu-us-privacy-shield-data-transfer-deal-faces-legal-challenge/ [hereinafter Lomas, *Legal Challenge*].

121 Goldstein et al., *supra* note 119, at 21. The European Union's General Data Protection Regulation will become effective on May 25, 2018. *See id.*

himself has commented on the deal saying "'[i]t's better than Safe Harbor, obviously, but far from what the ECJ has asked for.'"[122] As predicted, the Privacy Shield has already been challenged in court.[123] Despite the European Commission's view that the Privacy Shield is robust enough to comply with the European Data Protection Directive in Safe Harbor's place, it is unclear how the European Court of Justice will respond to the challenges raised.[124]

IV. PROPOSED SOLUTIONS: BUILDING TRUST & ESTABLISHING BASELINES

The cases discussed within this note establish that European courts are comfortable with examining and evaluating intelligence-gathering practices, intelligence agencies' activities and rationale, and their states' legal framework. The level of scrutiny and robust analysis undertaken by

122 Souppouris, *supra* note 120.

123 Julia Fioretti & Dustin Voltz, *Privacy Group Launches Legal Challenge Against EU-U.S. Data Pact*, REUTERS (Oct. 26, 2016, 1:25 PM), http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN12Q2JK. Digital Rights Ireland filed the legal challenge against the Privacy Shield although very few details are known about the case. Lomas, *Legal Challenge*, *supra* note 120. Digital Rights Ireland also was a party in *Maximillian Schrems v. Irish Data Protection Commissioner where their challenge successfully invalidated Safe Harbor. DRI Welcomes Landmark Data Privacy Judgment, DIGITAL RIGHTS IRELAND (Oct. 6, 2015),* https://www.digitalrights.ie/dri-welcomes-landmark-data-privacy-judgement/. *A French data rights group called La Quadrature du Net also filed suit, arguing the Privacy Shield should be annulled. Peter Sayer, A Second Privacy Shield Legal Challenge Increases Threat To EU-US Data Flows, PC WORLD (Nov. 3, 2016, 5:05 AM), http://www.pcworld.com/article/3138196/cloud-computing/a-second-privacy-shield-legal-challenge-increases-threat-to-eu-us-data-flows.html.*

124 In response to the challenge raised by Digital Rights Ireland, a European Commission spokesperson commented, "As we have said from the beginning, the Commission is convinced that the Privacy Shield will live up to the requirements set out by the European Court of Justice which has been the basis for the negotiations." Fioretti & Voltz, *supra* note 123. Max Schrems has challenged the Privacy Shield; he now is taking aim against the model clause provisions under the agreement. Glyn Moody, *In"An Unusual Move," US Government Asks to Join Key EU Facebook Privacy Case*, ARS TECHNICA (June 13, 2016), https://arstechnica.com/tech-policy/2016/06/eu-facebook-schrems-case-us-government-amicus-curiae/. The U.S. has joined the suit as amicus curie for the first time in an Irish court; the trade implications are huge. *Landmark EU-US Data Privacy Court Case Opens In Dublin*, RTÉ.IE (Feb. 7, 2017), https://www.rte.ie/news/2017/0207/850760-schrems-facebook-data/ [hereinafter RTÉ.IE]. Perhaps the European Court of Justice's previous ruling in *Schrems I* (which struck down Safe Harbor) pushed the U.S. to intervene in this latest challenge. Again, Maximillian Schrems challenges the adequacy of U.S. laws in protecting Facebook users from government surveillance. Moody, *supra*. This latest challenge, *Schrems II*, provides a tremendous opportunity for the U.S. government. The United States is expected to argue that since *Schrems I*, new enhanced protections safeguard EU citizens' privacy rights, and serious economic harm could occur if the European or Irish courts found otherwise. RTÉ.ie, *supra.* Regardless of the outcome, this case will place the U.S. government on the record without the protection of U.S. confidentiality laws. Moody, *supra.* Mr. Schrems believes this opportunity will provide greater insight into current U.S. surveillance practices because, "[n]ow they [the U.S.] have every chance to make their point, but we also have every chance to ask questions they have *previously not had to respond to*." Moody, *supra* (emphasis added).

European courts has not only been critical to our current understanding of data protection but also has revealed the inadequacies and thin protection available for citizens within Five Eyes nations, particularly for those within the United States.[125] This note advances three potential solutions that promote greater accountability and oversight within and among Five Eyes nations. First, this note encourages greater scrutiny by U.S. courts in evaluating the executive branch's practices and rationale when national security is provided as the basis for its surveillance operations. Second, this note proposes increased transparency and responsibility between U.S. lawmakers and its national intelligence community.

A. Less Deference to National Security as a Government Interest

When it comes to national security, cases before American courts often experience "national security exceptionalism."[126] In 1936, Justice George Sutherland quoted John Marshall's statement that "[t]he President is the sole organ of the nation in its external relations, and its sole representative with foreign nations."[127] This language has contributed to the development of the President's "independent and unchecked…foreign affairs power."[128] Accordingly, it is not surprising that courts regularly defer to the Executive Branch in matters regarding foreign relations.[129] Article II of the U.S. Constitution assigns the President the title of "Commander in

125 *See* James B. Rule, Opinion, *When it Comes to Protecting its Citizens' Data, Europe is Way Ahead Of The U.S.*, L.A. Times (May 12, 2014, 6:54 PM), http://www.latimes.com/opinion/op-ed/la-oe-rule-nsa-privacy-european-union-20140513-story.html.

126 This note borrows the term from Professors Ganesh Sitaraman and Ingrid Weurth to neatly refer to the rationale that "all national security cases as a group should be subject to different analysis than cases not related to national security…[because] courts should defer to the executive branch because the courts lack expertise in the field of national security, or because national security issues are uniquely important." Ganesh Sitaraman & Ingrid Weurth, *National Security Exceptionalism and the Travel Ban Litigation*, LAWFARE (Oct. 12, 2017, 3:00PM), https://www.lawfareblog.com/national-security-exceptionalism-and-travel-ban-litigation.

127 U.S. v. Curtiss-Wright Exp. Corp., 299 U.S. 394, 318 (1936).

128 Edward A. Purcell Jr., *Understanding Curtiss-Wright*, 31 L. & HIST. REV. 653, 653 (2013). *See Curtiss-Wright*, 299 U.S. at 319-20 (stating that the "authority vested in the President by an exertion of legislative power…plus the very delicate, plenary and exclusive power… as the sole organ of the federal government in the field of international relations" entitles the President to deference). *See also generally* Louis Fisher, *The Staying Power of Erroneous Dicta: From* Curtiss-Wright *to* Zivotofsky, 19 CONST. COMMENT. 149 (2016) (arguing that the *Curtiss-Wright* court's "sole organ" language has been misunderstood and misapplied to impermissibly enlarged the president's power over external affairs).

129 Curtis A. Bradley, Chevron *Deference and Foreign Affairs*, 86 VA. L. REV. 649, 659 (2000); *see also* Dep't of Navy v. Egan, 484 U.S. 518, 530 (1988) ("[U]nless Congress specifically has provided otherwise, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs.").

Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual Service of the United States."[130] This constitutional role along with Justice Sutherland's opinion have served as presidential justifications for unilateral authority in U.S. foreign affairs.[131] International conflicts in the twenty-first century pushed American presidents to use the Executive Branch as an "international policeman"[132] to protect U.S. interests. [133] The same concerns for increased efficiency, greater difficulty in identifying national security threats, and the need for proactive protection against these targets motivated the expansion of executive power [134] today.[135] When executive actions are legally challenged and national security is a proffered state rationale, "national security exceptionalism" sometimes influences courts to defer to the state's judgment.[136] This deference insulates executive action in the realm of international intelligence, necessary to defend national security against global threats,[137] from meaningful judicial scrutiny.[138] Moreover, agencies acting in the interest of national security receive deference due to their institutional expertise.[139]

Critics are right to push back against broad deference shielding

130 U.S. CONST., art. II § 2, cl. 1.

131 David Gartner, *Foreign Relations, Strategic Doctrine, and Presidential Power*, 63 ALA. L. REV. 499, 530-33 (2012).

132 *Id.* at 531.

133 *Id.*

134 *Id.* at 532-33 (quoting President Truman's response to the Supreme Court opinion in *Youngstown Sheet & Tube Co. v. Sawyer*).

135 *See President Trump on Syria Strikes: Full Transcript and Video*, N.Y. TIMES (Apr. 13, 2018), https://www.nytimes.com/2018/04/13/world/middleeast/trump-syria-airstrikes-full-transcript.html (stating that the April 2018 precision strikes on Syria are to end chemical warfare following the post -World War I effort to deter such security threats). *But see* Donald Trump (@realDonaldTrump), TWITTER (Aug. 20, 2013, 4:02 PM), https://twitter.com/realDonaldTrump/status/373581528405905408 ("The President must get Congressional approval before attacking Syria-big mistake if he does not!").

136 "[T]he Supreme Court has stated in no uncertain terms that "[i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation... [and] we have previously invoked 'our traditional deference to the judgment of the executive department in matters of foreign policy.'" United States v. Ghailani, 733 F.3d 29, 47 (2d Cir. 2013) (quoting *Haig v. Agee*, 453 U.S. 280, 307 (1981)).

137 *See supra* note 39.

138 Michael P. Fix & Kirk A. Randazzo, *Judicial Deference and National Security: Applications of the Political Question and Act of State Doctrines*, 6 DEMOCRACY & SEC. 1, 13 (2010).

139 Anjali S. Dalal, *Shadow Administrative Constitutionalism and the Creation of Surveillance Culture*, 2014 MICH. ST. L. REV. 61, 115 (2014). *See also* Holder v. Humanitarian Law Project, 561 U.S. 1, 34 (2010) (quoting Rostker v. Goldbery, 453 U.S. 57, 65 (1981)) ("[W]hen it comes to collecting evidence and drawing factual inferences in [national security and foreign relations], 'the lack of competence on the part of the courts is marked.'").

government action from robust judicial review when national security is raised as a governmental interest.[140] Greater analysis by courts of the intelligence agencies' activities provides "incentives for greater democratic responsiveness" from executive agencies.[141] Such institutional analyses would also inform "courts' deference with greater predictability" and also incentivize democratic accountability by improving accountability with judicial oversight[142] as seen in the European challenges to governmental surveillance.[143]Additionally, increased discussions by courts as to what specific factors lead to justified deference would provide greater legal clarity while maintaining the integrity of national security concerns.[144] However, there are substantial judicial barriers preventing such institutional analyses, limiting the creation of judicial oversight.[145] The judicial doctrine surrounding the President's Article II powers and executive privilege require additional, coinciding reforms to empower courts to engage in such an analysis.[146]

B. Placing Responsibility on Congress

Another takeaway from the European courts' handling of government surveillance cases is the key role that the data protection framework of the European Union plays in creating both legal and procedural safeguards for individuals' data. Both European judges and lawmakers contribute to the

---

140 *See, e.g.*, Ilya Somin, Opinion, *The Case Against Special Judicial Deference in Immigration And National Security Cases*, WASH. POST (Oct. 22, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/10/22/the-case-against-special-judicial-deference-in-immigration-and-national-security-cases/?utm_term=.11b53f0e3602; *see also* Jack M. Blakin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 23 (2008).

> If the executive seeks greater efficiency, this requires a corresponding duty of greater disclosure before the fact and reporting after the fact to determine whether its surveillance programs are targeting the right people or are being abused. Judges must also counter the executive's increasing use of secrecy and the state secrets privilege to avoid accountability for its actions. Executive officials have institutional incentives to label their operations as secret and beyond the reach of judicial scrutiny. Unless legislatures and courts can devise effective procedures for inspecting and evaluating secret programs, the Presidency will become a law unto itself.

Id.

141 Eric Berger, Deference Determinations and Stealth Constitutional Decision Making, 98 IOWA L. REV. 465, 522 (2013)

142 Id. at 523.

143 See supra text accompanying notes 74-80, 107-117.

144 Berger, supra note 141, at 525. See id. at 520-33, for an in-depth discussion of the advantages and limitations of judicial analyses of governmental agencies' behavior and processes when making more specific deference determinations.

145 Dalal, supra note 139, at 133.

146 Id. at 132-33.

data protection regime, as should their American counterparts. American lawmakers have similarly accepted the executive's judgment in foreign relations and intelligence.[147] Similarly, Congress has avoided opportunities to curb the executive's expanding privilege to withhold national security information from courts and Congress.[148] Congress's failure to ensure that the civilian supremacy of the military is balanced between itself and the executive contravenes the Constitution, republican government, and liberalism.[149]

In order to effectively limit a magnified executive power[150] and legislate in matters concerning government surveillance and foreign relations, Congress must then also have "access to national security information."[151] Such access will also support courts' ability to protect litigants' rights and "judicial subservience to executive interests."[152] In addition to requiring access to national security information, Congress must examine the current legal framework surrounding intelligence-gathering and government surveillance. For instance, "[i]n its advice-and-consent role, the Senate has taken ambassadorial and national security nominees as political hostages" undermining U.S. representation oversees and leadership in executive agencies.[153] Additionally, lawmakers are uninformed about "the foreign policy, defense, and intelligence issues on which they vote."[154] Likewise, Congress suffers from a number of institutional and political obstacles[155]– national security committees remain structured as they did during the Cold War,[156] fail to appreciate the relative complexity of cross-jurisdictional issues in a globalized political climate,[157] neglect to oversee the intelligence community,[158] and lack

147 See Sarah Fowler, Note, Circumventing the Constitution for National Security: An Analysis of the Evolution of the Foreign Intelligence Exception to the Fourth Amendment's Warrant Requirement, 4 U. MIAMI NAT'L SECURITY & ARMED CONFLICT L. REV. 207, 223 (2014) (discussing Congress's failure to regulate intelligence surveillance).

148 See Louis Fisher, Congressional Access to National Security Information, 45 HARV. J. ON LEGIS. 219, 220-21 (2008).

149 Id. at 221-22.

150 Purcell, supra 128.

151 Fisher, supra note 148, at 234.

152 Id.

153 KAY KING, COUNCIL ON FOREIGN REL., CONGRESS AND NATIONAL SECURITY 6 (2010).

154 Id. at 7.

155 Id. at vii.

156 Id. at 15.

157 Id. at 16.

158 Id.

commitment to diplomacy.[159] The Constitution tasks Congress to oversee the Executive's intelligence work, and Congress must take this responsibility seriously. Indeed, "[t]he solution to a lack of congressional oversight is conceptually easy but practically difficult."[160] Congress must both legislate and regularly exercise its authority to oversee the intelligence community, two assignments that require "significant political power and effort."[161]

V. CONCLUSION

Both *Schrems I* and *II*, along with *10 Human Rights Organizations v United Kingdom*, illustrate how legal challenges that attack the *transfer* of data between Five Eyes countries protect privacy effectively. These legal battles democratize the decisions that have been made about government surveillance with the help of judicial oversight working hand-in-hand with a legal framework that addresses government surveillance.

The globalization of national security efforts makes it extremely difficult to ensure individual rights are not being violated, undermining the legitimacy of international intelligence.[162] A legislative solution working with judicial review of national surveillance can provide the necessary oversight to ensure transparency and accountability. However, if Americans care about data privacy, Congress needs to maintain a broader, global perspective of the surveillance landscape. International information-sharing has been largely unchecked,[163] and while the privacy debate surrounding national surveillance regimes has become more robust post-Snowden,[164] "the privacy risks posed by *global* information sharing" have been absent from the conversation.[165] While Snowden may not have been enough,[166] perhaps the current interest in data protection, surveillance, and its use by foreign governments can promote oversight, accountability, and transparency over national security surveillance through judicial and congressional responsibility.[167] Surveillance needs democratic governance

159 Id. at 20.
160 Dalal, supra note 139, at 135.
161 Id. at 134.
162 McGruddy, supra note 10, at 215-16.
163 Kim, supra note 7.
164 Id.
165 Id.
166 Dalal, supra note 139, at 135.
167 See Copy That: America Should Borrow From Europe's Data-Privacy Law, ECONOMIST (Apr. 5, 2018), https://www.economist.com/news/leaders/21739961-gdprs-premise-consumers-should-

desperately, but before we can ensure that the intelligence community respects the constitutional and legislative limits surrounding their operations, the U.S. needs to recognize that global intelligence-sharing must also have oversight, accountability, and transparency.

Rachel C. Taylor[*]

---

be-charge-their-own-personal-data-right; Jamie Metzl & Eleonore Pauwels, Is America's National Security Facebook and Google's Problem?, TECHCRUNCH (Apr. 15, 2018), https://techcrunch.com/2018/04/15/is-americas-national-security-facebook-and-googles-problem/ (Senator Bill Nelson stated, "If Facebook and other online companies will not or cannot fix the privacy, then we are going to have to. We, the Congress.").

* Executive Notes Editor, Washington University Global Studies Law Review, J.D. (2018), Washington University School of Law, B.A. (2014), University of South Florida.