2013

NSA Surveillance Since 9/11 and the Human Right to Privacy

G. Alex Sinha
Maurice A. Deane School of Law at Hofstra University

NSA SURVEILLANCE SINCE 9/11 AND THE HUMAN RIGHT TO PRIVACY

*G. Alex Sinha**

ABSTRACT

Since shortly after 9/11, if not earlier, the National Security Agency (NSA) has been collecting massive amounts of data about American citizens and permanent residents, ostensibly with the aim of preempting future terrorist attacks. While the NSA's program has invited substantial scholarly attention, specifically concerning its compliance with the United States Constitution and various domestic statutes, the academic debate about its merits entirely omits one crucial fact: the United States is also legally obliged to protect a human right to privacy, as codified in Article 17 of the International Covenant on Civil and Political Rights (ICCPR). This Article seeks to eliminate the blind spot caused by that omission, illustrating the relevance of human rights for assessing the legality and propriety of NSA surveillance. It argues that even under conservative assumptions about the scope of the NSA program and the coverage of the ICCPR, there is good reason to think that the program violates the covenant. At the very least, as this detailed case study of the NSA program demonstrates, more clarity from the Human Rights Committee on the right to privacy is essential in a world characterized by increasing government surveillance.

Section I of this Article provides a brief history of domestic

* Aryeh Neier Fellow, Human Rights Watch and the American Civil Liberties Union. The research for and writing of this Article took place prior to my affiliation with HRW or the ACLU, and the views expressed here do not necessarily reflect the positions of either organization. I am deeply grateful to Philip Alston for his valuable input throughout the process of researching and writing this Article. I am also thankful to Smita Narula, Faiza Patel, and Ira Rubinstein for their excellent comments, as well as to audiences at the April 2013 Emerging Human Rights Scholarship Conference and the 2012–13 International Human Rights Clinic (both at New York University School of Law). All errors are my own.

spying in the United States, leading up to and through the passage of the Foreign Intelligence Surveillance Act of 1978 (FISA). FISA constituted the first major legislative effort to regulate the electronic surveillance of American citizens or permanent residents within the United States for foreign intelligence or international counterterrorism purposes, and Section I concludes by outlining the key provisions of this landmark statute. Section II traces the chronology of revelations about the NSA program and relevant statutory developments, starting with the original disclosure of the program in December of 2005 and ending with revelations made in August of 2013. Section III of the Article explains why Article 17 of the ICCPR applies with full force to the United States, while Section IV unpacks some of the language of Article 17 to illustrate why its provisions apply to the activities of the NSA. Finally, Section V explores several ways in which the NSA program appears to violate the provisions of Article 17.

INTRODUCTION

As of 2010, the National Security Agency (NSA) was collecting and storing nearly two billion emails, phone calls, and other communications every day,[1] as well as countless points of transactional data, all as part of a surveillance program that remains in place. Many of these communications and data points exclusively concern Americans suspected of no wrongdoing whatsoever.[2] It is quite possible that current domestic law

1. Dana Priest & William Arkin, *A Hidden World, Growing Beyond Control*, WASH. POST, July 19, 2010, at 3, http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/3/. It is difficult to locate more recent data on that point, though in March 2013 alone, the NSA apparently gathered nearly 100 billion pieces of information from worldwide computer networks, with three billion coming from United States computer networks. Glenn Greenwald & Ewen MacAskill, *Boundless Informant: the NSA's secret tool to track global surveillance data*, GUARDIAN (June 11, 2013, 9:00 PM), http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining.

2. *See, e.g.*, Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, GUARDIAN, June 5, 2013 [hereinafter Greenwald, *NSA collecting phone records*], http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (detailing the government's ongoing collection of all of Verizon's calling records completely irrespective of the government's level of suspicion of Verizon customers); Glenn Greenwald & James Ball, *The top secret rules that allow NSA to use US data without a warrant*, GUARDIAN, June 20, 2013, http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant (describing the government's ability to review and use the communications of Americans collected inadvertently).

(amended repeatedly since 9/11) permits the NSA to do at least some of this, ostensibly with the aim of protecting the United States from future terrorist attacks.[3] Domestic legal changes notwithstanding, this Article asks whether and how international human rights law (as codified in the International Covenant on Civil and Political Rights, or ICCPR) bears on the domestic surveillance activities of the NSA—a question that has gone all but ignored in the debate about the NSA program that began when the *New York Times* first revealed the secret program in December of 2005.[4] The Article concludes that the NSA program is worrisome from a human rights standpoint, and calls on international human rights bodies to clarify and emphasize the right to privacy.

CONTEXT

In December of 2005, the *New York Times* reported that President Bush had authorized the NSA to eavesdrop on domestic phone calls and collect private emails without court-approved warrants.[5] According to the *Times*, President Bush authorized the program in a secret 2002 executive order.[6] The *Times* also reported that it had possessed documentation of the NSA program for months before running the article but had held off from publishing it under pressure from the Bush Administration.[7] The article spurred some members of Congress to attempt to conduct oversight of the program,[8] and the

---

3. *See* Greenwald, *NSA collecting phone records*, *supra* note 2 (describing the breadth of the government's efforts to collect purely domestic transactional data, as authorized by the Foreign Intelligence Surveillance Court under the "business records" provision of the USA PATRIOT Act); *cf.* Letter from Am. Civil Liberties Union to the U.S. Senate (June 25, 2008) [hereinafter ACLU Letter], *available at* http://www.aclu.org/images/general/asset_upload_file902_35782.pdf (arguing that the FISA Amendments Act "unconstitutionally and unnecessarily permits the government to vacuum up international communications, without a connection . . . even to national security").

4. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all (offering the first public description of any part of this surveillance program).

5. *Id.*

6. *Id.*

7. *Id.*

8. *See* Douglas Jehl, *Among Those Told of Program, Few Objected*, N.Y. TIMES, Dec. 23, 2005, http://www.nytimes.com/2005/12/23/politics/23intel.html?_r=1& (suggesting that sudden public attention focused on the NSA program, which began with the original *New York Times* story, served as a catalyst for a variety of oversight

disclosure of the program introduced a new element into the ongoing debate about the difficulties of protecting both national security and civil liberties. The *Times* article also sparked an outcry from those concerned that the NSA program was illegal.[9] Indeed, over the past few years, scholars have repeatedly analyzed the known elements of the NSA program under domestic legislation (like the Foreign Intelligence Surveillance Act) and the United States Constitution. Concerns about the program's compliance with domestic statutes have led to substantial revisions of federal surveillance laws—for example, to inoculate major telecommunication companies from civil liability for their complicity in the program[10] and to relax restrictions on the collection of foreign-to-foreign communications that pass through the United States.[11]

But the United States also has international legal obligations, which have been almost completely overlooked in the NSA controversy. Though it is generally reluctant to bind itself under human rights treaties,[12] the United States ratified the International Covenant on Civil and Political Rights (ICCPR) in

---

attempts).

9. *See, e.g.*, Glenn Greenwald, *Finally punishing the wrongdoers in the NSA scandal*, UNCLAIMED TERRITORY BLOG (Dec. 30, 2005, 3:53 PM), http://glenngreenwald.blogspot.com/2005/12/finally-punishing-wrongdoers-in-nsa.html (referring to the program as "illegal" a mere two weeks after the *New York Times* revealed it).

10. Pamela Hess, *Senate Immunizes Telecom Firms From Wiretap Lawsuits*, N.Y. SUN, July 9, 2008, http://www.nysun.com/national/senate-grants-telecom-companies-immunity/81525/.

11. Ellen Nakashima & Joby Warrick, *House Approves Wiretap Measure*, WASH. POST, Aug. 5, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/08/04/AR2007080400285.html?nav=rss_politics.

12. *See* International Covenant on Economic, Social & Cultural Rights, Oct. 5, 1977, 993 U.N.T.S. 3, *available at* https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-3&chapter=4&lang=en (indicating that the United States has signed but not ratified the International Covenant on Economic, Social & Cultural Rights, a treaty with 161 parties); Convention on the Elimination on All Forms of Discrimination against Women, July 17, 1980, 1249 U.N.T.S. 13, *available at* https://treaties.un.org/pages/viewdetails.aspx?src=treaty&mtdsg_no=iv-8&chapter=4&lang=en (indicating that the United States has signed but not ratified the Convention on the Elimination on All Forms of Discrimination against Women, a treaty with 187 parties); Convention on the Rights of the Child, Feb. 16, 1995, 1577 U.N.T.S. 3, *available at* https://treaties.un.org/Pages/ViewDetails.aspx?mtdsg_no=IV-11&chapter=4&lang=en (indicating that the United States has signed but not ratified the Convention on the Rights of the Child, a treaty with 193 parties).

1992.[13] Article 17 of the ICCPR codifies a human right to privacy, and at the very least, questions arise as to whether the NSA program violates that right.[14] The lack of debate about the relationship between the NSA program and the United States' human rights obligations may in part reflect a deeper problem: that human rights bodies have not addressed the issue of electronic surveillance in sufficient detail to clarify state obligations surrounding activities like those currently ongoing in the United States. Additionally, there remain numerous important questions about the precise size and shape of the NSA program, complicating any assessment of whether the program is compatible with the ICCPR.

Nevertheless, the question is an important one. Having chosen to bind itself to the terms of the ICCPR, gaining whatever public relations and political benefits such a choice entails, the United States may not simply disregard the attendant legal obligations. If it turns out that the United States is violating the terms of Article 17, then only a series of very specific conditions could allow the United States to escape the conclusion that it is in violation of its human rights obligations. As it happens, those conditions—relating to derogation under the terms of the ICCPR, to blanket inapplicability of the treaty, or to reservations, understandings and declarations (RUDs) attached by the United States to the relevant article of the ICCPR—do not obtain in this case.[15] Thus, in essence, if the NSA program violates the protections laid out in the ICCPR, then the United States is also violating its human rights obligations.[16]

---

13. International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, S. Exec. Doc. E, 95-2, 999 U.N.T.S. 171 [hereinafter ICCPR], *available at* https://treaties.un.org/pages/viewdetails.aspx?src=treaty&mtdsg_no=iv-4&chapter=4&lang=en (documenting the United States' ratification of the Covenant on June 8, 1992).

14. *Id.* ("No one shall be subjected to arbitrary or unlawful interference with his privacy . . . .").

15. The United States has, however, declared that the substantive articles of the ICCPR are not "self-executing," which means that individuals protected by the treaty cannot seek judicial enforcement of the treaty's provisions against the United States without additional domestic legislation licensing such judicial action. *See* ICCPR, *supra* note 13 (detailing the United States' position on self-execution).

16. While a state may generally violate a treaty that is not self-executing without triggering the full range of consequences considered typical of domestic legal transgressions, states tend to contest allegations of human rights abuses in vigorous terms. Allegations of human rights violations implicitly carry strong normative condemnation and form the grounds for wide-ranging criticism from individuals, civil

This conclusion, if warranted, would be significant for at least two reasons. First and foremost, human rights treaties and covenants are designed to prevent human rights violations. Accordingly, as a normative matter, we should not simply abide human rights violations without any public debate in those terms and without an explicit (and legitimate) justification from the violator. The United States has argued that the program is legal under domestic law—though many commentators and some federal judges have disagreed. To the best of my knowledge, however, the government has not explained in any detail why the program is legal under the ICCPR.[17]

Moreover, if it is illegal, given the apparent scope of the NSA program, the number of violations of the human right to privacy could easily climb into the millions, billions, or even trillions.[18] The extensive and systematic nature of the program could thus compel the conclusion that the United States is violating the human right to privacy within its borders on a truly colossal scale.

I. THE ORIGINAL LEGAL FRAMEWORK FOR DOMESTIC SURVEILLANCE IN THE UNITED STATES

Analysis of the relevant terms of the ICCPR will be most useful later, following an exposition of the details of the NSA program; however, a brief review of Article 17 will help to reveal what information is necessary to undertake a proper analysis and will thus help to provide a form for the ensuing investigation. Article 17 of the ICCPR comprises two clauses. Article 17(1) states: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence,

---

society groups, and other states. It would be an extremely surprising result for the U.S. to concede human rights violations on the ground that it cannot necessarily be held accountable by a court for those violations.

17. In 2011, the government submitted its Fourth Periodic Report of the United States of America to the United Nations Committee on Human Rights Concerning the International Covenant on Civil and Political Rights. Its discussion of Article 17 refers to the NSA program, but entirely glosses over why such a program would be permissible under the terms of the ICCPR. *See* U.S. DEP'T OF STATE, FOURTH PERIODIC REPORT OF THE UNITED STATES OF AMERICA TO THE UNITED NATIONS COMMITTEE ON HUMAN RIGHTS CONCERNING THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS ¶¶ 321-35 (Dec. 30, 2011), *available at* http://www.state.gov/j/drl/rls/179781.htm#art17. Additional research has turned up no further explanation from the government of the legality of the program under international human rights law.

18. *See infra* text accompanying notes 347-354.

nor to unlawful attacks on his honour and reputation."[19] Article 17(2) adds: "Everyone has the right to protection of the law against such interference or attacks."[20] For our immediate purposes, it suffices to note that "unlawful" in this context encapsulates (but is not exhausted by) activities that contravene domestic law,[21] which suggests that understanding the domestic legal framework for conducting surveillance is essential to the present analysis. To illustrate that framework, the following Section provides a brief history of the primary operative statute governing surveillance for the purposes of gathering foreign intelligence and combating international terrorism—the Foreign Intelligence Surveillance Act of 1978—before tracing the outlines of the NSA program and more recent legislative developments that have modified the law.

A. A BRIEF HISTORY OF 20TH CENTURY DOMESTIC SURVEILLANCE IN THE UNITED STATES

The Foreign Intelligence Surveillance Act of 1978 (FISA) arose out of perceived government surveillance abuses that largely began around the 1930s.[22] It constituted the first comprehensive legislative response to the privacy concerns raised by public revelations about the scope of domestic surveillance that had occurred under various presidents (from both parties) beginning in the early-to-mid-twentieth century.[23] Technological advances started to make it easier for the government to monitor people, whether they were located abroad or at home.[24] Until the 1960s and early 1970s—when the public and the courts first began to confront in earnest the issue of domestic surveillance[25]—the government took full advantage of its growing capacity to spy.

---

19. ICCPR, *supra* note 13, art. 17(1).

20. ICCPR, *supra* note 13, art. 17(2).

21. *See* MANFRED NOWAK, U.N. COVENANT ON CIVIL AND POLITICAL RIGHTS: CCPR COMMENTARY 382 (2d rev. ed. 2005) (interpreting the meaning of "lawful" in just this way).

22. *See* US SENATE SELECT COMMITTEE ON INTELLIGENCE ACTIVITIES WITHIN THE UNITED STATES, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS: 1976 US SENATE REPORT ON ILLEGAL WIRETAPS AND DOMESTIC SPYING BY THE FBI, CIA AND NSA 16 (1976) [hereinafter CHURCH COMMITTEE REPORT] (noting that warrantless wiretapping began to occur frequently in the 1930's).

23. *See* text accompanying notes 22-44 (providing numerous examples).

24. CHURCH COMMITTEE REPORT, *supra* note 22, at 239 (describing the technological capabilities at the time of FISA's passage). Obviously, modern technological developments have increased the capacity for spying.

25. There are some modest exceptions, but not enough to undermine the point.

Between 1947 and 1973, as part of its SHAMROCK Program, the government collected and turned over to the NSA millions of telegrams that originated within, terminated in, or traveled through the United States.[26] Some of these telegrams constituted purely citizen-to-citizen correspondence (telegrams sent by Americans to other Americans).[27] Senders were never notified that the government had collected their telegrams, and telegraph company executives who assisted with the program received assurance that they would not be prosecuted because the program was "'in the highest interests of the nation.'"[28]

Sometime in the early 1960s, the NSA began to assemble "watch lists" that contained the names of American citizens.[29] Originally designed to track those traveling to Cuba as well as those who might pose a danger to the President and other high-level officials, by the fall of 1967, the watch list program had morphed into a systematic attempt to track Americans who might be involved in civil disturbances—with a focus on civil rights and antiwar groups.[30] In 1969, the NSA implemented Project MINARET, which tightened the security around its watch list program and expanded its scope.[31] Under President Nixon, MINARET grew to cover approximately 300,000 targets.[32]

The Federal Bureau of Investigation (FBI) also participated in domestic surveillance during this era. It began to undertake some measure of warrantless wiretapping in 1931, and continued almost without pause at least through 1975.[33] During that time, the scope of FBI surveillance was especially broad, though a few representative highlights will suffice for present purposes. For example, during this era and as part of the FBI's COMINFIL (communist infiltration) Program, the FBI conducted substantial surveillance of the NAACP for approximately twenty-five years—

---

26. CHURCH COMMITTEE REPORT, *supra* note 22, at 119. The Church Committee describes a slightly different range of dates later in its report. *See id.* at 407 (pegging the SHAMROCK Program down to the years between 1945 and 1975).

27. *Id.* at 120.

28. *Id.* at 104.

29. *Id.* at 392.

30. *Id.* at 392-93.

31. CHURCH COMMITTEE REPORT, *supra* note 22, at 395-96.

32. GABRIEL SCHOENFELD, NECESSARY SECRETS: NATIONAL SECURITY, THE MEDIA, AND THE RULE OF LAW 37 (2010).

33. CHURCH COMMITTEE REPORT, *supra* note 22, at 242 (summarizing the approach of all three branches to the FBI's warrantless surveillance, from the program's inception up until the writing of the report).

notwithstanding both the agency's own "initial finding that the NAACP was opposed to communism" and the agency's continued inability to locate any evidence to the contrary.[34]

The FBI also developed COINTELPRO (counterintelligence program), which was "designed to 'disrupt' groups and 'neutralize' individuals deemed to be threats to domestic security."[35] It was under the auspices of COINTELPRO that the FBI vigorously employed a wide range of surveillance techniques to discredit civil rights leader Martin Luther King, Jr.[36] At one point, the FBI shared one of its surveillance tapes with Dr. King, with the stated goal (according to at least one agent) of destroying his marriage. They also sent a note that "Dr. King and his advisors interpreted as a threat to release the tape unless Dr. King committed suicide."[37]

The Central Intelligence Agency (CIA) was involved in domestic surveillance during this era as well.[38] Between 1940 and 1973, the CIA and FBI secretly—and illegally, according to an investigating Senate committee[39]—"opened and photographed first class letter mail within the United States"[40] with the purpose of collecting "foreign intelligence and counterintelligence information."[41] Over that span, the two agencies implemented twelve separate programs that involved opening private mail and recording its contents,[42] and copies of that correspondence remained on-hand at least through 1976.[43] The collective scope of the programs is difficult to discern, but apparently just one of these programs collected and photographed over 215,000 pieces of correspondence.[44]

---

34. CHURCH COMMITTEE REPORT, *supra* note 22, at 125.

35. *Id.* at 14.

36. *Id.* at 14-15.

37. *Id.* at 15.

38. In listing programs run by the NSA, FBI, and CIA, I do not mean to imply that these were the only organizations involved in performing surveillance on Americans. Instead, I have simply attempted to capture a representative cross-section of the operative programs to show the widespread nature of domestic surveillance. As discussed below, even the U.S. Army was involved in such activities during the 1970s.

39. CHURCH COMMITTEE REPORT, *supra* note 22, at 294.

40. *Id.*

41. *Id.* at 295.

42. *Id.* at 294.

43. *Id.* at 295 (noting that the letters "are retained even today").

44. CHURCH COMMITTEE REPORT, *supra* note 22, at 295.

Although the foregoing list does not provide an exhaustive account of the domestic intelligence activities that were later disclosed to the public—indeed, there are many more—it provides a clear and representative picture of the sort of activities that arose before FISA passed into law. These programs remained more or less secret until the mid-1970s, but public awareness of domestic surveillance issues begin to grow in 1970, when Christopher Pyle revealed that while serving in the Army, he learned of a military program designed to keep tabs on "politically suspect" Americans (using some 1,500 plainclothes Army intelligence agents to monitor all demonstrations in the United States that involved twenty or more people).[45] Senator Sam Ervin (a Democrat representing North Carolina) began investigating that program, which allegedly started under President Johnson; however, uncooperative Army leadership apparently stymied Ervin's inquiries for more information.[46]

On March 8, 1971, several Vietnam War protesters broke into an FBI field office in Pennsylvania, in search of proof that the agency was illegally monitoring left-wing activists.[47] They stole hundreds of documents, some of which substantiated the concerns behind their break-in.[48] Over the next several months, the burglars mailed select documents from the stolen cache to several journalists, including Betty Medsger at the Washington Post.[49] The Post then published a series of articles based on the documents, revealing "how the F.B.I. was spying on political activists and actively trying to disrupt their activities."[50]

Then, in 1972, the Watergate scandal broke, generating

---

45. *An Impeachable Offense? Bush Admits Authorizing NSA to Eavesdrop on Americans Without Court Approval*, DEMOCRACY NOW (Dec. 19, 2005) [hereinafter *An Impeachable Offense?*], http://www.democracynow.org/2005/12/19/an_impeachable_offense_bush_admits_authorizing.

46. *See* Karl E. Campbell, *Senator Sam Ervin and the Army Spy Scandal of 1970-71: Balancing National Security and Civil Liberties in a Free Society*, CHARLOTTE-MECKLENBURG HISTORIC LANDMARKS COMMISSION, http://www.cmhpf.org/Random%20Files/senator%20sam%20ervin.htm (last visited Feb. 3, 2014) (describing the Army cover-up in response to Ervin's inquiries).

47. Bonnie Bertram & Drew Magratten, *The FBI File Heist That Changed History*, DAILY BEAST (Jan. 7, 2014), http://www.thedailybeast.com/articles/2014/01/07/the-fbi-file-heist-that-changed-history.html.

48. *Id.*

49. *Id.*

50. *Id.*; *see* BETTY MEDSGER, THE BURGLARY: THE DISCOVERY OF J. EDGAR HOOVER'S SECRET FBI (2014).

widespread media attention.[51] And in 1974, reporting by Seymour Hersh revealed that the CIA had engaged in (among other things) widespread domestic surveillance of antiwar groups and political dissidents during the Nixon Administration. That program, known as "Operation CHAOS," was discussed in a series of internal CIA reports, colloquially known as the Family Jewels.[52] The momentum created by this chain of events, linked prominently by their temporal proximity, forced concern about the activities of spy agencies to a critical mass in the Senate.[53]

In early 1975, the Senate voted to create the eleven-man[54] Senate Select Committee to Study Governmental Operations with

---

51. LOCH K. JOHNSON, A SEASON OF INQUIRY: THE SENATE INTELLIGENCE INVESTIGATION 11 (1985).

52. Seymour Hersh, *Huge C.I.A. operation reported in U.S. against antiwar forces, other dissidents in Nixon years*, N.Y. TIMES, Dec. 22, 1974; *see also* U.S. SENATE, JANUARY 27, 1975 CHURCH COMMITTEE CREATED [hereinafter U.S. SENATE, CHURCH COMMITTEE CREATED], http://www.senate.gov/artandhistory/history/minute/Church_Committee_Created.htm (last visited Feb. 3, 2014) (describing the effect of the Hersh article); JOHNSON, *supra* note 51, at 9-10 (doing the same). Some have pointed to other factors that contributed to an environment conducive to investigations of the intelligence community. These include concerns among the public about the execution of the Vietnam War and allegations that the intelligence community had been attempting to destabilize foreign governments. JOHNSON, *supra* note 51, at 11.

53. JOHNSON, *supra* note 51, at 11. There were other contemporaneous investigations as well, which were not conducted by the Senate. At the very beginning of 1975, President Ford created a commission headed by Vice President Nelson Rockefeller to look specifically at the activities of the CIA. *Id.* at 10-11. Many regarded that as an unsuccessful attempt to preempt congressional investigations that would be less accountable to the executive branch. *See id* at 10. The House also established a pair of investigating committees, with Lucien Nedzi (Democrat of Michigan) serving as the chair of the first. FRANK JOHN SMIST, CONGRESS OVERSEES THE UNITED STATES INTELLIGENCE COMMUNITY: 1947-1994, at 137 (2d ed. 1994). When that committee imploded six months into its mandate, the House created a replacement led by Otis Pike, Democrat of New York. *Id.* at 152-53. Yet even Pike's committee fared poorly, receiving criticism for hostility toward the intelligence community, unprofessionalism, and an inability to protect confidential information. *See generally id.* at 153-213. The House voted to allow the executive branch to censor Pike's final report, and an uncensored version only reached the public via unauthorized leaks to the press. *Id.* at 169-71. The entire debacle turned the House off from intelligence oversight—in contrast to the Senate, which drew on its reasonably favorable experience with Church to establish a permanent oversight panel with considerably more stability. *Id.* at 214. It is for these reasons that I focus on Church and his committee's findings.

54. All members of the committee—six Democrats and five Republicans—were male. *See* JOHNSON, *supra* note 51, at 14 (providing names and photographs of all members).

Respect to Intelligence Activities[55]—now commonly known as the "Church Committee" for its Chair, Frank Church (a Democrat from Idaho).[56] The Committee took its mandate to center primarily around "whether intelligence activities threaten 'the rights of Americans.'"[57] It issued a number of reports, with one in particular detailing most of the activities summarized above (as well as many more programs left aside for the purposes of this Article).[58] The Church Report roundly condemned the behavior of intelligence agencies on the whole, finding that:

> [T]he targets of intelligence activity have ranged far beyond persons who could properly be characterized as enemies of freedom and have extended to a wide array of citizens engaging in lawful activity. . . . Unless new and tighter controls are established by legislation, domestic intelligence activities threaten to undermine our democratic society and fundamentally alter its nature.[59]

The forceful conclusions of the Church Committee, and the attendant push for regulation of the surveillance activities of United States intelligence agencies, led to the passage of the Foreign Intelligence Surveillance Act of 1978.[60]

B. THE PASSAGE OF FISA

The scandals that led up to the formation of the Church Committee, and the revelations contained in the Church Report, proved sufficient impetus for the creation of a strong legal framework regulating government surveillance activities. President Carter signed FISA into law in 1978,[61] establishing legislative guideposts regulating all electronic surveillance of

---

55. *See Select Committee to Study Governmental Operations with Respect to Intelligence Activities ("Church Committee")*, U.S. SENATE SELECT COMMITTEE ON INTELLIGENCE, http://www.intelligence.senate.gov/churchcommittee.html (last visited Feb. 3, 2014).

56. *See* U.S. SENATE, CHURCH COMMITTEE CREATED, *supra* note 52 (giving the full name of the committee).

57. CHURCH COMMITTEE REPORT, *supra* note 22, at 7.

58. *See generally id.* (providing the text of what I refer to here as the "Church Committee Report").

59. *Id.* at 7.

60. *See* GLENN GREENWALD, HOW WOULD A PATRIOT ACT?: DEFENDING AMERICAN VALUES FROM A PRESIDENT RUN AMOK 24 (2006) (making explicit the link between the work of the Church Committee and the passage of FISA). The text of the statute is available at 50 U.S.C. § 1801 (2012).

61. GREENWALD, *supra* note 60, at 24.

American citizens or permanent residents within the United States for foreign intelligence or international counterterrorism purposes.[62] Under FISA, the government retains broad powers to engage in electronic surveillance; however, when eavesdropping on the domestic or international communications of American citizens or permanent residents, government officials must operate under at least a modicum of judicial oversight lest they be guilty of a felony.[63]

Specifically, FISA created the Foreign Intelligence Surveillance Court (FISC, or FISA court), a "secret" court whose deliberations take place with only the government present, but whose approval is necessary for extended surveillance of Americans.[64] One newspaper has characterized the role of the FISC as follows: "The court is meant to approve all wiretaps placed inside America for intelligence-gathering purposes."[65]

The FISC meets at the Justice Department.[66] Its function, as suggested above, is to evaluate the government's requests for warrants for conducting surveillance on American citizens and permanent residents. FISA directs the FISC to authorize warrants where there is "probable cause to believe that the target of surveillance is an agent of a foreign state or a terrorist group,"[67] and the standard of proof appears to be lower than the standards in typical criminal proceedings.[68] The FISC nearly always accedes to government requests: "[F]rom 1978 to 2001—the year President Bush ordered [the NSA to begin operating outside of the FISA framework]—the government submitted a total of 13,102 requests to the . . . court to eavesdrop on Americans." The court requested modifications to just two of these requests, and ultimately approved them all.[69]

---

62. GREENWALD, *supra* note 60, at 24, 26.

63. *See id* at 25-26. FISA caps the penalty for violations at $10,000 in fines and five years in prison. *Id.* at 26 (citing 50 U.S.C. § 1809(c)).

64. *See* Philip Shenon, *Secret Court Says F.B.I. Aides Misled Judges in 75 Cases*, N.Y. TIMES, Aug. 23, 2002, http://www.nytimes.com/2002/08/23/us/secret-court-says-fbi-aides-misled-judges-in-75-cases.html?pagewanted=all (noting that the court generally operates in secret).

65. Hess, *supra* note 10.

66. Risen & Lichtblau, *supra* note 4.

67. GREENWALD, *supra* note 60, at 26 (citing 50 U.S.C.A. § 1805(a) (2008)).

68. Risen & Lichtblau, *supra* note 4.

69. GREENWALD, *supra* note 60, at 28. The Electronic Privacy Information Center has extracted similar statistics from what appear to be the same source: reports compiled by the Federation of American Scientists. *See* ELEC. PRIVACY INFO. CTR.,

Though the FISC can grant emergency surveillance approval within a matter of hours,[70] FISA also recognized the possibility that urgent circumstances might require the government to begin surveillance before there is time to secure the permission of the FISC. Thus, FISA at one point permitted the government to conduct surveillance of Americans for up to seventy-two hours without a warrant.[71] (That period has since been extended to 168 hours.)[72] In times of war, the warrantless provision becomes even more generous, permitting the government to engage in surveillance (related to gathering foreign intelligence information) for up to fifteen days before securing permission from the FISC.[73]

These provisions were intended to make it possible for the government to continue conducting surveillance as needed for the purposes of protecting national security. At the same time, by introducing some measure of judicial review, the law had the potential to screen out the use of intelligence agencies for purely political purposes, a rampant problem under previous administrations[74] that arguably reached its apex in Watergate. To achieve this purpose, FISA built in stringent criminal penalties for anyone who violated its terms: under § 1809, the law mandates up to five years in prison and $10,000 in fines for any official who "engages in electronic surveillance under color of law except as authorized [under FISA]."[75]

The fact that FISA emerged during the Cold War—a crisis that was plausibly of substantially greater proportions than the one the United States faces presently in terrorism—may be significant, at least for interpreting what sorts of countervailing

---

FOREIGN INTELLIGENCE SURVEILLANCE ACT COURT ORDERS 1979-2011, http://epic.org/privacy/wiretap/stats/fisa_stats.html (last updated May 4, 2012). According to their statistics, between 1970 and 2011, there were only eleven rejected FISA applications out of thousands submitted (with all of the rejections occurring in 2003 or later). ELEC. PRIVACY INFO. CTR., FOREIGN INTELLIGENCE SURVEILLANCE ACT COURT ORDERS 1979-2011, http://epic.org/privacy/wiretap/stats/fisa_stats.html (last updated May 4, 2012).

70. Risen & Lichtblau, *supra* note 4.

71. 50 U.S.C.A. § 1805(f).

72. *See* 50 U.S.C.S. § 1881a(g)(1)(B) (2008) (codifying the shift to seven days).

73. *Id.*

74. *See supra* text accompanying notes 29-37, 45-52 (describing some of the more striking examples of politically-motivated surveillance in the U.S. during the 20th century).

75. 50 U.S.C. § 1809(a)(c).

considerations (if any) the legislators behind the law would have accepted as trumping its provisions.[76] As Glenn Greenwald has pointed out: "In the year FISA was enacted, the Soviet empire had multiple nuclear warheads aimed at scores of American cities."[77] Given the context and FISA's explicit wartime provisions, it does not appear that the existence of threats from foreign powers or terrorist groups would, alone, suffice to justify bypassing the law.[78]

II. TRACING THE ARC OF THE NSA PROGRAM

A. REVELATION OF THE NSA PROGRAM[79]

The NSA program has evolved since its inception, as has what we know about it. Many of the details are difficult to ascertain because of the secret nature of the program and discrepancies in what has been reported, including the conflicting accounts given by whistleblowers and active, high-ranking government officials. We can begin by laying out what is presently known about the NSA program and describing updates to the domestic legal framework since 9/11.

There is a bit of ambiguity about when the program began.

---

76. GREENWALD, *supra* note 60, at 26-27 (discussing the political and national security context at the time of FISA's passage and comparing that to more recent circumstances).

77. *Id.* at 26.

78. *See id.* at 26-28 (implying the same conclusion by noting that Congress chose to include judicial oversight requirements on FISA-regulated surveillance practices notwithstanding the magnitude of the national security threat posed at the time by the Soviet Union).

79. Throughout this Article, I will use the term "NSA program" to refer broadly to the expanded surveillance activities of the NSA that have been disclosed in the wake of 9/11, beginning with warrantless surveillance of domestic-to-foreign communications in (at least) late 2001. The program has, at various points, publicly been referred to as the "Terrorist Surveillance Program" (or TSP), as well (internally at the NSA) as Operation Stellar Wind. *See, e.g.*, Siobhan Gorman, *NSA's Domestic Spying Grows As Agency Sweeps Up Data*, WALL ST. J. (Mar. 10, 2008, 12:01 AM) [hereinafter Gorman, *NSA's Domestic Spying*], http://online.wsj.com/public/article/SB120511973377523845.html?mod=blog (giving the former name); James Bamford, *The NSA Is Building The Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 15, 2012, 7:24 PM) [hereinafter Bamford, *NSA Spy Center*], http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1 (using the latter name). For simplicity, I will avoid both of these names. At the same time, different parts of what I refer to as the "NSA program" appear to fall into discrete programs under the NSA's own internal classification (such as PRISM, Boundless Informant, and so on) and thus my use of the term is not felicitous in a formal sense.

According to some sources, President Bush signed the executive order that authorized the program in 2002,[80] but the program itself appears to have started days after the attacks on September 11, 2001.[81] One explanation for this timing discrepancy appears in a 2008 *Wall Street Journal* article, according to which the NSA may originally have implemented the program by relying on an outstanding executive order from the early 1980s before receiving an updated authorization order from President Bush in 2002.[82]

In any case, the first public report of the program appeared on the front page of the *New York Times* on December 16, 2005.[83] The *Times* reported that the NSA had begun eavesdropping on people within the United States—some of them Americans—without warrants and that the NSA had derived its authority to begin this program under an order signed by President Bush in 2002.[84] According to the *Times*, up to 500 people within the United States (and 5,000 to 7,000 abroad) were subject to warrantless surveillance at any given point, though the total number of people who had been affected by the program over its life was substantially larger because the list of targets changed over time.[85] Both phone calls and email were targeted under the program, though the aim was to pursue only calls and emails with at least one point of contact (origination or termination)

---

80. *See, e.g.*, Risen & Lichtblau, *supra* note 4 (providing this information); Dan Eggen, *Bush Authorized Domestic Spying*, WASH. POST, Dec. 16, 2005, http://www.washingtonpost.com/wpdyn/content/article/2005/12/16/AR2005121600021.html (doing the same).

81. Eggen, *supra* note 80 (noting an official's comments that "[t]he effort . . . began days after the [9/11] attacks"); *see also* Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA TODAY (May 11, 2006, 10:38 AM) http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm ("The NSA's domestic program began soon after the Sept. 11 attacks . . . .").

82. *See* Gorman, *NSA's Domestic Spying*, *supra* note 79 ("In response to the Sept. 11 attacks, then NSA-chief Gen. Michael Hayden has said he used his authority to expand the NSA's capabilities under a 1981 executive order governing the agency. Another presidential order issued shortly after the attacks, the text of which is classified, opened the door for the NSA to incorporate more domestic data in its searches, one senior intelligence official said.").

83. *See* Risen & Lichtblau, *supra* note 4 (the article itself). Later reporting suggests that the original leak to the *Times* began with a Republican lawyer from the Justice Department named Thomas Tamm. *See* Joe Conason, *A whistle-blower who needs Obama and Holder's protection*, SALON (Apr. 17, 2009, 5:39 AM), http://www.salon.com/2009/04/17/whistleblower_2/.

84. Risen & Lichtblau, *supra* note 4.

85. *Id.*

abroad.[86]

The *Times* reported that the program began to accelerate in 2002, when the CIA started to detain greater numbers of terrorism suspects.[87] The government sought to begin surveillance immediately on individuals who were linked in some way to these suspects—for instance, individuals whose contact information appeared in the suspects' phones or computers.[88] Even as of 2005, however, during initial reporting on the program, the *Times* noted that the government still required FISC warrants for monitoring purely domestic communications (as opposed to communications between someone within the United States and someone abroad).[89]

The initial report also noted that the program may have undergone changes in the middle of 2004, when federal judge Colleen Kollar-Kotelly (the federal judge who oversaw the FISC at the time) complained that the government might be misusing information gathered without warrants.[90] The details of the complaint have not been reported publicly, but the idea appears to be that the government was bootstrapping its way to warrant requests before the FISC by relying in those requests on information gathered via warrantless NSA surveillance—a practice that Judge Kollar-Kotelly appeared to find unacceptable.[91] Resulting changes included the first audit of the program by the Justice Department, as well as the department's development of a more detailed checklist for identifying whether the NSA should undertake surveillance of particular targets.[92]

These are the key facts that the public confronted in its first brush with the NSA program. Yet there is a legitimate question as to what exactly prompted the government to begin the program in the first place. Because the secret order by President Bush that authorized the program was promulgated in 2002 and the program is thought to have started shortly after the 9/11 attacks, it is natural to think of those attacks as the catalyst

86. Risen & Lichtblau, *supra* note 4.
87. *Id.*
88. *Id.*
89. *Id.*
90. *Id.*
91. Risen & Lichtblau, *supra* note 4.
92. *Id.*

behind the introduction of the program.[93] Indeed, some government officials have said that the expanded surveillance only began after the attacks,[94] and one common name for the program is the "Terrorist Surveillance Program" (TSP).[95]

But there is some indication that the NSA began expanding its surveillance activities (or at least laying the groundwork to do so) months before 9/11. According to Joseph Nacchio, the former CEO of Qwest Communications, the NSA began applying pressure on Qwest in February of 2001 to secure its cooperation in a surveillance program that Qwest's lawyers regarded as illegal.[96] It may be worth noting that these accusations came out as Nacchio fought (ultimately unsuccessfully) against charges of insider trading; however, Nacchio's defense team supported its claims by pointing out similar allegations in an earlier lawsuit.[97] These allegations suggested that about seven months before the 9/11 attacks, AT&T had begun preparing a facility specifically for the NSA to use in gaining access to the phone and Internet information on AT&T's network.[98] Additional details, however, remain difficult to ascertain.

Leaving aside difficult questions about the months directly leading up to 9/11, we can piece together a few important facts based on what had been reported before the program was

---

93. *See, e.g.*, Risen & Lichtblau, *supra* note 4 (linking the program to 9/11).

94. *See, e.g.*, Scott Shane, *Former Phone Chief Says Spy Agency Sought Surveillance Help Before 9/11*, N.Y. TIMES, Oct. 14, 2007, http://www.nytimes.com/2007/10/14/business/14qwest.html?ref=todayspaper (noting that multiple government officials have said the warrantless wiretapping only started after 9/11, under an order from President Bush); James Bamford, *The NSA is still listening to you*, SALON (July 22, 2009, 5:19 AM) [hereinafter Bamford, *NSA is listening*], http://www.salon.com/2009/07/22/eavesdropping_2/ (claiming that the "administration's decision to open the NSA's surveillance floodgates [came] following the 9/11 attacks").

95. *See* Gorman, *NSA's Domestic Spying*, *supra* note 79 (referring to the program as the "Terrorist Surveillance Program). This is the name used to describe the original instantiation of the program, which (without warrants) collected calls and emails between domestic and international parties. *See, e.g.*, Am. Civil Liberties Union v. Nat'l Sec. Agency, 493 F.3d 644 (6th Cir. 2007) (using the abbreviation "TSP" to refer to the program in its original form).

96. Shane, *supra* note 94.

97. *Id.*; *see also* Andrew Harris, *Spy Agency Sought U.S. Call Records Before 9/11, Lawyers Say*, BLOOMBERG (June 30, 2006, 6:46 PM), http://www.bloomberg.com/apps/news?pid=newsarchive&sid=abIV0cO64zJE (advancing the same allegations regarding AT&T's alleged involvement in the NSA's surveillance program).

98. Shane, *supra* note 94.

disclosed and what was reported in the *New York Times*'s December 16, 2005 bombshell. For one, we know that after the 9/11 attacks, the Bush Administration began to push publicly for expanded powers to fight terrorism.[99] One result—signed into law mere weeks after the attacks, on October 26—was the Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001 (the USA PATRIOT Act).[100]

The USA PATRIOT Act, among many other things, explicitly revised FISA to make it easier for the government to conduct surveillance under the FISA framework.[101] It amended FISA in several key ways, including allowing for "roving" warrants that applied to all phones used by a particular target rather than to specific phone numbers[102] and permitting intelligence agencies to share among themselves the information that they secured through such eavesdropping.[103]

Several commentators have observed that while the Bush Administration was publicly pushing for the USA PATRIOT Act, in part with the aim of easing FISA's requirements, it simultaneously and secretly initiated the NSA program, which ignored that framework altogether.[104] Whatever its legal significance, this was clearly a deliberate approach by the Bush Administration, inasmuch as President Bush publicly declared the USA PATRIOT Act's FISA modifications sufficient for fighting terrorism.[105]

B. A Summary of Subsequent Developments Concerning the NSA Program

Following the initial disclosure of the NSA program on December 16, 2005, a general pattern began to emerge in subsequent reporting: periodically, articles would appear in various media outlets indicating that the NSA program was

---

99. *E.g.*, GREENWALD, *supra* note 60, at 12.

100. USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

101. *Id.*

102. *Id.* § 206.

103. *Id.* § 203.

104. *See* GREENWALD, *supra* note 60, at 14 (observing this feature of the timing); Risen & Lichtblau, *supra* note 4 (doing the same).

105. GREENWALD, *supra* note 60, at 13 (alleging this after President Bush noted "[t]his new law . . . will allow surveillance of all communications used by terrorists . . .").

actually larger than originally disclosed.[106] As of the writing of this Article, that pattern had continued to grow stronger as a result of the ongoing publication of leaks from Edward Snowden.[107] While those trends may be a function of more information about the program simply leaking out over time, they could also reflect the expanding nature of the program, the latter being consistent with strong patterns in spying activities uncovered by the Church Committee.[108]

Just five days after running its first article on the program, the *Times* followed up with a report that some purely domestic calls had been intercepted because of a technical "glitch."[109] More specifically, some calls between two parties in the United States had apparently been intercepted when the NSA mistakenly concluded that one of the parties to the call happened to be located abroad.[110]

The joint effect of these first NSA articles was to spur a flurry of activity in Congress in early 2006, as various legislative branch officials sought to placate concerned constituents by learning more about the program while simultaneously toeing the executive branch's aggressive line on preserving secrecy around the government's counterterrorism efforts.[111] Much of the resistance in Congress ultimately led nowhere in the face of

---

106. *See* Cauley, *supra* note 81 (showing this trend); Gorman, *NSA's Domestic Spying*, *supra* note 79 (the same); *see also infra* text accompanying notes 109, 157, 163, and 202-237 (the same).

107. *See infra* text accompanying notes 109-118, 130-138, and 157-237 (documenting this pattern).

108. *See* CHURCH COMMITTEE REPORT, *supra* note 22, at 9 ("The tendency of intelligence activities to expand beyond their initial scope is a theme which runs through every aspect of our investigative findings.").

109. *See* James Risen & Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. TIMES, Dec. 21, 2005 [hereinafter Risen & Lichtblau, *Spying Program*], http://www.nytimes.com/2005/12/21/politics/21nsa.html?ex=1292821200&en=91d434311b0a7ddc&ei=5088&partner=rssnyt&emc=rss&_r=0 (first reporting these facts).

110. *Id.* Note that General Hayden's quote on the matter seemed to contradict the *Times* story directly: "'The authorization given to N.S.A. by the president requires that one end of these communications has to be outside the United States,' General Hayden answered. 'I can assure you, by the physics of the intercept, by how we actually conduct our activities, that one end of these communications are always outside the United States.'" *Id.*

111. *See generally* Tara M. Sugiyama & Marisa Perry, *The NSA Domestic Surveillance Program: An Analysis of Congressional Oversight During an Era of One-Party Rule*, 40 U. MICH. J.L. REFORM 149 (2006) (describing the oversight climate in Congress as it first publicly confronted the NSA program).

strong pressure from the Bush administration.[112]

On April 7, 2006, *Wired Magazine* published the public statement of Mark Klein, who had spent over twenty-two years as a technician with AT&T.[113] Klein alleged that AT&T had cooperated with the NSA in creating "splitter cabinets" that would allow for the monitoring of all Internet and phone traffic routed through facilities in several major American cities.[114] One month later, in May of 2006, *USA TODAY* reported that the NSA program was actually much larger than previously acknowledged by the government, as AT&T, Verizon, and BellSouth (with 200 million customers among them) had been working under contract with the NSA to provide an enormous amount of transactional data about the domestic phone call patterns of American citizens.[115] As the article put it, the "government has detailed records of calls . . . made [by customers of these telecommunication companies]—across town or across the country—to family members, co-workers, business contacts and others."[116]

The information turned over by the telecom companies apparently omitted certain personal details about the callers—names, addresses, and the like—but the article noted that the NSA has the power to locate that information with ease, simply by cross-checking the phone numbers against other information in its possession.[117] The authors also quoted an anonymous source as saying that the program involved "the largest database ever assembled in the world," and they noted that previous assurances by President Bush that the NSA was focusing on foreign calls misleadingly suggested to Americans that their domestic calling information was secure.[118]

---

112. *See* Sugiyama & Perry, *supra* note 111, at 166 (noting that congressional oversight was, on the whole, ineffective).

113. *See generally Wiretap Whistle-Blower's Account: Statement of Mark Klein*, WIRED, Apr. 6, 2006, http://www.wired.com/science/discoveries/news/2006/04/70621.

114. *See id.* (providing Klein's explicit allegations). Klein subsequently provided evidence for a lawsuit over the NSA program, undertaken by the Electronic Frontier Foundation. *See* ELEC. FRONTIER FOUND., *NSA Spying on Americans*, https://www.eff.org/issues/nsa-spying/ (last visited Feb. 3, 2014) (noting Klein's participation in the suit).

115. Cauley, *supra* note 81.

116. *Id.*

117. *Id.*

118. *Id.*

In late July of 2007, claiming that "[o]ur national security depend[ed] on it," President Bush used a radio address to call for further revision or modernization of FISA.[119] He highlighted four changes to the FISA framework contained in a bill pending before Congress,[120] and he called for the bill's passage.[121] Congress obliged,[122] and on August 5, 2007, President Bush signed into law the Protect America Act of 2007 (PAA).[123] The PAA granted the government the power to collect foreign communications that "pass through communication nodes on U.S. soil."[124] More controversially, the PAA was designed to make it easier to conduct surveillance all around, in part by reducing the role of the FISC to approving target selection parameters in general rather than actually authorizing particular surveillance via warrants.[125] Under the PAA, the latter authority was vested in the Attorney General and the Director of National Intelligence, who were empowered to issue yearlong warrants for the surveillance of people reasonably believed to be located outside the United States.[126] The law left it unclear how to handle

---

119. *See* President George W. Bush, President's Radio Address (July 28, 2007), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2007/07/print/20070728.html (providing text of the address).

120. *Id.* ("First, it brings FISA up to date with the changes in communications technology that have taken place over the past three decades. Second, it seeks to restore FISA to its original focus on protecting the privacy interests of people inside the United States, so we don't have to obtain court orders to effectively collect foreign intelligence about foreign targets located in foreign locations. Third, it allows the government to work more efficiently with private-sector entities like communications providers, whose help is essential. And fourth, it will streamline administrative processes so our intelligence community can gather foreign intelligence more quickly and more effectively, while protecting civil liberties.")

121. *See id.* ("Our intelligence community warns that under the current statute, we are missing a significant amount of foreign intelligence that we should be collecting to protect our country. Congress needs to act immediately to pass this bill, so that our national security professionals can close intelligence gaps and provide critical warning time for our country.").

122. *See* Nakashima & Warrick, *supra* note 11 (describing Congress's cooperation).

123. Juan P. Valdivieso, Recent Developments, 45 HARV. J. ON LEGIS. 581, 581 (2008), *available at* http://www3.law.harvard.edu/journals/jol/files/2013/10/581-600_Valdivieso-2008.pdf.

124. Nakashima & Warrick, *supra* note 11.

125. *See id.* ("Oversight by the Foreign Intelligence Surveillance Court . . . would be limited to examining whether the government's guidelines for targeting overseas suspects are appropriate.").

126. PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, HUMAN RTS. WATCH, COMMENTS OF HUMAN RIGHTS WATCH 5 (2013) [hereinafter COMMENTS OF HUMAN RIGHTS WATCH], *available at* http://www.hrw.org/sites/default/files/related_material/

incidental foreign communications (with one party located in the United States) that were captured in pursuing the targets of those long-term warrants.[127] Advocates praised the law for enabling the government to gather communications about its targets irrespective of where those communications originate.[128] Opposition to the bill from Democratic lawmakers managed to secure a single concession: a six-month sunset provision, which came into effect in early 2008, ending the PAA.[129]

On March 10, 2008, shortly after the PAA expired, Siobhan Gorman at the *Wall Street Journal* reported that NSA surveillance was broader still than previous disclosures had indicated, noting that "efforts [by the NSA to gather surveillance domestically] have evolved to reach more broadly into data about people's communications, travel and finances in the U.S. than the domestic surveillance programs brought to light since the 2001 terrorist attacks."[130] Gorman detailed the NSA's activities as relayed to her by "two former officials familiar with the data-sifting efforts."[131] They described the following operation:

> [The officials] work by starting with some sort of lead, like a phone number or Internet address. In partnership with the FBI, the systems then can track all domestic and foreign transactions of people associated with that item -- and then the people who associated with them, and so on, casting a gradually wider net.[132]

Citing an intelligence official, Gorman went on to provide an example of how the program could manifest:

> If a person suspected of terrorist connections is believed to be in a U.S. city -- for instance, Detroit, a community with a high concentration of Muslim Americans -- the government's spy systems may be directed to collect and analyze all

---

Comment%20HRW%20PCLOB%20Final%208-1-13_0.pdf.

127. *See ACLU Fact Sheet on the "Police America Act,"* AM. CIV. LIBERTIES UNION (Aug. 7, 2007), http://www.aclu.org/national-security/aclu-fact-sheet-%E2%80%9C police-america-act (documenting some concerns). The ACLU harshly criticized the law, referring to it as the "Police America Act" in a fact sheet it released two days after the PAA became law. *Id.*

128. Nakashima & Warrick, *supra* note 11.

129. *See id.*

130. Gorman, *NSA's Domestic Spying*, *supra* note 79.

131. *Id.*

132. *Id.*

> electronic communications into and out of the city.
>
> The haul can include records of phone calls, email headers and destinations, data on financial transactions and records of Internet browsing. The system also would collect information about other people, including those in the U.S., who communicated with people in Detroit.
>
> The information doesn't generally include the contents of conversations or emails. But it can give such transactional information as a cellphone's location, whom a person is calling, and what Web sites he or she is visiting. For an email, the data haul can include the identities of the sender and recipient and the subject line, but not the content of the message.[133]

Gorman reported that the legal argument for the permissibility of such a program hinges on the government's interpretation of a Supreme Court case from 1979, which allowed for the warrantless collection of phone call records.[134] While Gorman pointed out that several laws require court orders for transactional data, she also noted that the USA PATRIOT Act has generally made it easier to get such information.[135] Additionally, Gorman claimed that the NSA gains access to transactional data through the FBI, using "telecommunications hubs" like the one that caused former AT&T official Mark Klein to come forward with information in 2006.[136] Gorman noted that, in the Electronic Frontier Foundation lawsuit launched in connection with Klein's disclosures, "a former technology adviser to the Federal Communications Commission" speculated that there could be as many as twenty such stations around the United States.[137] Moreover, according to Gorman, "[c]urrent and former intelligence officials confirmed a domestic network of hubs, but didn't know the number."[138]

---

133. Gorman, *NSA's Domestic Spying*, *supra* note 79.

134. *Id.* The article does not identify the relevant case, but it appears to be *Smith v. Maryland*. *See generally* Smith v. Maryland, 442 U.S. 735 (1979) (holding that the use of "pen registers," installed on telephone company property with the aim of recording phone numbers dialed by customers, did not require a warrant because callers automatically turn over their calling records to the phone company and thus lose their expectation of privacy in the numbers they dial).

135. Gorman, *NSA's Domestic Spying*, *supra* note 79.

136. *Id.*

137. *Id.*

138. *Id.*

On July 10, 2008, President Bush signed into law the final major amendment to the FISA framework.[139] The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISA Amendments Act, or FAA) stood in for the 2007 PAA, which had expired in February as a result of its six-month sunset provision.[140] One major provision, which garnered substantial press coverage in the weeks leading up to the passage of the FAA, extended retroactive immunity to telecom companies that had been assisting the NSA in collecting data without the involvement of the FISC.[141] The effect of that provision was to head off almost four-dozen pending lawsuits against telecoms for their involvement in surveillance that violated FISA.[142]

The law ostensibly imposed several surveillance restrictions that were missing under the PAA (though as Glenn Greenwald has pointed out, the February 2008 expiration of the PAA meant that in the interim, until the FAA became law, the applicable law simply reverted back to the original FISA framework as modified largely through the USA PATRIOT Act).[143] First, under the FAA, the FISC has the exclusive authority to issue warrants for targeted surveillance of Americans overseas based on some degree of probable cause—a power that the PAA had controversially granted to the Attorney General and the Director of National Intelligence.[144] (The FAA requires FISC warrants for targeting Americans abroad.)[145] The law also requires annual

---

139. It is final as of February 2014, though future changes remain possible.

140. Glenn Greenwald, *Obama's new statement on FISA*, UNCLAIMED TERRITORY BLOG (July 3, 2008) [hereinafter Greenwald, *Obama on FISA*], http://utdocuments.blogspot.com.br/2008/07/obamas-new-statement-on-fisa.html. The FAA was renewed at the end of 2012, so it remains applicable today, though it is set to expire again, barring renewal, in 2017. *Obama Signs FISA Warrantless Wiretapping Program Extension Into Law*, HUFFINGTON POST (Dec. 30, 2012, 5:49 PM), http://www.huffingtonpost.com/2012/12/30/obama-fisa-warrantless-wiretapping_n_2385690.html.

141. *See, e.g.*, Kit Bond, *FISA Amendments Act of 2008*, WALL ST. J. (June 19, 2008, 6:24 PM), http://online.wsj.com/article/SB121391360949290049.html (noting this liability protection extends up until "the President's Terrorist Surveillance Program was brought under the FISA Court"; Hess, *supra* note 10; Paul Kane, *House Passes Spy Bill; Senate Expected to Follow*, WASH. POST, June 21, 2008, http://www.washingtonpost.com/wpdyn/content/story/2008/06/20/ST2008062001087.html (noting that immunity depends on showing "written assurance from the Bush administration that the spying was legal").

142. Hess, *supra* note 10.

143. Greenwald, *Obama on FISA*, *supra* note 140.

144. COMMENTS OF HUMAN RIGHTS WATCH, *supra* note 126; Hess, *supra* note 10.

145. Hess, *supra* note 10.

submissions from the Attorney General and the Director of National Intelligence to the FISC, detailing the government's surveillance targeting provisions and seeking the court's approval for those provisions applicable to the targeting of foreigners outside the United States.[146]

The FAA also reconfirms the FISA framework as the exclusive means for engaging in domestic wiretapping for intelligence purposes,[147] though that is not necessarily a useful provision. For one, the previous FISA framework, with its original exclusivity provision, came back into effect in February 2008.[148] Moreover, the breadth of the FAA may obviate the purported need for the NSA to work outside the law.[149]

More controversially, the law gave the Director of National Intelligence and the Attorney General joint power to grant broad, yearlong warrants for targeting foreign people or groups.[150] This provision raised major concerns among critics. One was that Americans suspected of no wrongdoing, and for whose communications no warrants had been granted, would have their correspondence swept up incidentally in broad investigations of "true" targets.[151] The other major concern was that the FISC retained too small a role in overseeing the targeting of foreigners.[152] As with the PAA, under the FAA the FISC does not issue warrants with respect to correspondents believed by intelligence officials to be both non-American and outside the United States; instead, the statute limits the role of the court to reviewing the targeting and minimization procedures that the

---

146. 50 U.S.C.S. § 1881a (2008).

147. Bond, *supra* note 141; Hess, *supra* note 10.

148. Greenwald, *Obama on FISA*, *supra* note 140.

149. *See* Marty Lederman, *The Key Questions About the New FISA Bill*, BALKINIZATION (June 22, 2008, 8:27 PM), http://balkin.blogspot.com/2008/06/key-questions-about-new-fisa-bill.html (expressing the idea that the law might be so permissive as to render extra-legal operations of the NSA unnecessary).

150. *See* COMMENTS OF HUMAN RIGHTS WATCH, *supra* note 126 (summarizing key provisions of the FAA).

151. *See, e.g.*, ACLU Letter, *supra* note 3, at 2 (expressing this concern where the real target is abroad but an American is "on the other end of those communications"). According to former Department of Justice lawyer David Kris, this is indeed the way the government has interpreted the FAA. Lederman, *supra* note 141 (interviewing David Kris). This is a point we will return to below. *See infra* text accompanying notes 211-218.

152. *See, e.g.*, COMMENTS OF HUMAN RIGHTS WATCH, *supra* note 126 (expressing precisely this concern).

Attorney General and the Director of National Intelligence use to select targets falling within that category.[153]

The FAA also expanded the "emergency," pre-warrant surveillance window (from 72 to 168 hours, or one week),[154] and it created a large exigency loophole that permits common use of the pre-warrant provision.[155] Finally, the law empowers the government to continue surveillance of targets even if the FISC rejects the applications submitted for those targets; such "unauthorized" surveillance can continue for as long as sixty days during the FISC appeals process.[156]

Several meaningful reports about the scope of the program followed the passage of the FAA. In April of 2009, the *New York Times* revealed that the NSA had "intercepted private e-mail messages and phone calls of Americans in recent months on a scale that went beyond the broad legal limits established by Congress [in the FAA] . . . ."[157] The *Times* suggested that the problem became apparent during the FAA certification process described above, which requires the Attorney General and Director of National Intelligence to submit surveillance protocols for approval by the FISC.[158] The *Times* also suggested that the over-collection of data may have been unintentional, at least in part the result of difficulties in distinguishing "between communications inside the United States and those overseas as [the NSA] uses its access to American telecommunication companies' fiber-optic lines and its own spy satellites to intercept millions of calls and e-mail messages."[159] Additionally, the article noted independent allegations of misconduct leveled against the NSA by a senior FBI agent, whose information suggested that the NSA might be targeting Americans for surveillance based on

153. *See* ACLU Letter, *supra* note 3, at 3 (summarizing these concerns).

154. Hess, *supra* note 10.

155. ACLU Letter, *supra* note 3, at 4. "The bill permits the government to start a spying program and wait to go to court for up to 7 days every time 'intelligence important to national security of the US may be lost or not timely acquired.'" *Id.* As the letter notes, all court applications take some time, and under the language provided, it is unclear if "even a 30 minute delay" could be deemed as "impeding 'timely' acquisition." *Id.*

156. *Id.* at 5.

157. Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. TIMES, Apr. 15, 2009, http://www.nytimes.com/2009/04/16/us/16nsa.html?pagewanted=1&_r=0.

158. *Id.*

159. *Id.*

insufficient evidence of their ties to terrorism.[160] In one instance, the NSA had apparently attempted—without a warrant—to listen in on the conversations of a congressman during a 2005 or 2006 trip to the Middle East (though the *Times* claimed that the proposal to do so was ultimately rejected).[161]

In June of 2009, the *Times* followed up again.[162] It reported that the government claimed to have corrected the problems identified in the paper's April article, but that more information had surfaced about the possibility that the NSA had, since at least 2005, been examining large volumes of Americans' emails without warrants.[163] More specifically, the *Times* claimed that the NSA had overstepped its FISC authorization in eight to ten different court orders, which could have resulted in millions of improperly collected individual communications.[164] According to the *Times*, the FAA was passed partly to ease the NSA's task in collecting email correspondence, but the NSA had been using a large email database called "Pinwale" since at least 2005, accessing Americans' emails (without warrants) in the process.[165] The *Times* quoted a former NSA analyst as saying that "Pinwale allowed N.S.A. analysts to read large volumes of e-mail messages to and from Americans as long as they fell within certain limits—no more than thirty percent of any database search, he recalled being told—and Americans were not explicitly singled out in the searches."[166]

In 2010, the *Washington Post* reported further on the scope of the program, claiming that each day the NSA would "intercept and store 1.7 billion e-mails, phone calls and other types of communications."[167] According to the *Post*, one result of the massive scale of that program was that the government was struggling with the logistical challenges of managing so much

160. Lichtblau & James Risen, *supra* note 157.

161. *Id.* ("The official said the plan was ultimately blocked because of concerns from some intelligence officials . . . .").

162. James Risen & Eric Lichtblau, *E-Mail Surveillance Renews Concerns in Congress*, N.Y. TIMES, June 16, 2009, [hereinafter Risen & Lichtblau, *E-Mail Surveillance*], http://www.nytimes.com/2009/06/17/us/17nsa.html?pagewanted=all&_r=0.

163. *Id.*

164. *Id.*

165. *Id.*

166. *Id.*

167. Priest & Arkin, *supra* note 1.

data; the NSA program alone required the agency to feed its data into seventy different databases.[168]

Then, in March of 2012, James Bamford published an article in *Wired Magazine* about the NSA's construction of a massive data storage facility in Bluffdale, Utah.[169] His report included schematics for the compound and described the groundbreaking ceremony for the project, which occurred in early 2011.[170] The compound is expected to house, among other things, a "1-million-square-foot data storehouse" capable of storing the digital equivalent of 500 quintillion pages of text.[171]

For his 2012 article, Bamford also spoke on the record for the first time with an NSA "crypto-mathematician" named James Binney. Binney had worked at the NSA for nearly forty years and had been deeply involved in setting up parts of its surveillance apparatus.[172] However, he resigned in 2001—shortly after warrantless wiretapping began—because he believed the program to violate the Constitution.[173]

Binney claimed that the NSA had placed its telecom wiretapping switches so as to gain access to domestic communications when it was physically possible to place the switches differently and thereby restrict access solely to foreign communications.[174] He also claimed that the NSA program, codenamed "Stellar Wind," involved the inspection of both domestic phone calls and domestic emails.[175] Days later, the director of the NSA, General Keith Alexander, testified before Congress; in response to questions that were based on revelations in Bamford's article, Alexander denied that the agency has the

168. Priest & Arkin, *supra* note 1.

169. *See* Bamford, *NSA Spy Center*, *supra* note 79 (giving a detailed account of the project). Bamford first reported on plans to build the Utah Data Center for Salon in July of 2009. Bamford, *NSA is listening*, *supra* note 94 (containing Bamford's earlier reporting on the project).

170. *See* Bamford, *NSA Spy Center*, *supra* note 79.

171. *Id.* In numerical form, "500 quintillion" appears as a five followed by twenty zeroes (500,000,000,000,000,000,000). *Id.*

172. *Id.*

173. *Id.*

174. *Id.* (explaining that the agency could simply have placed its stations where the fiber-optic cables come ashore, rather than at "key junction points throughout the country").

175. Bamford, *NSA Spy Center*, *supra* note 79.

capacity to record purely domestic calls or emails.[176] Bamford posted a rejoinder the following day.[177]

Binney claimed that the program initially recorded about 320 million calls per day and that it only got larger from there; with the participation of major telecoms like AT&T and Verizon, Binney said the program was gathering over 1.5 billion calls per day.[178] Between 2001 and 2012, he estimated that the NSA had gathered fifteen to twenty trillion communications.[179] He also claimed that NSA's taps, located in various secret rooms around the country, can scan Internet traffic based on remote directions issued from the NSA's headquarters in Fort Meade, Maryland.[180] Those taps utilize software that can search "for target addresses, locations, countries, and phone numbers, as well as watch-listed names, keywords, and phrases in email."[181] As Bamford put it: "Any communication that arouses suspicion, especially those to or from the million or so people on agency watch lists, are automatically copied or recorded and then transmitted to the NSA."[182] Additionally, Binney also confirmed "that the NSA gained warrantless access to AT&T's vast trove of domestic and international billing records."[183]

Binney claims to have suggested a system for monitoring communications that would have correlated the degree of

---

176. *See* Andy Greenberg, *NSA Chief Denies Wired's Domestic Spying Story (Fourteen Times) in Congressional Hearing*, FORBES (Mar. 20, 2012, 8:31 PM), http://www.forbes.com/sites/andygreenberg/2012/03/20/nsa-chief-denies-wiredsdomesticspying-story-fourteen-times-in-congressional-hearing/ (describing Alexander's testimony). The next day, Bamford responded, suggesting that the NSA often issues denials that employ a technical definition of common words: for example, the NSA can deny that it intercepts certain communications in cases where the layperson might disagree because "'[i]ntercept,' in NSA's lexicon, only takes place when the communications are 'processed' 'into an intelligible form intended for human inspection,' not as they pass through NSA listening posts and [are] transferred to data warehouses." James Bamford, *NSA Chief Denies Domestic Spying But Whistleblowers Say Otherwise*, WIRED (Mar. 21, 2012, 2:37 PM) [hereinafter Bamford, *Whistleblowers*], http://www.wired.com/threatlevel/2012/03/nsa-whistleblower/all/.

177. *See* Bamford, *Whistleblowers*, *supra* note 176 (offering Bamford's response to Alexander).

178. Bamford, *NSA Spy Center*, *supra* note 79.

179. *Id.*

180. *Id.*

181. *Id.*

182. *Id.*

183. Bamford, *NSA Spy Center*, *supra* note 79.

scrutiny of a given person with proximity to the target.[184] Thus, as the degrees of separation between the NSA's target and another person increased, the amount of information about that person that would be captured would decrease.[185] But Binney said that the NSA rejected his suggestion at the time, and now the agency may simply be collecting everything it can.[186] Moreover, Binney told Bamford that the agency could chart a person's activities on a graph, even including information about that person's financial transactions and travel plans.[187] He also claimed that the NSA can eavesdrop on and record calls in real time, an allegation corroborated by another one of Bamford's sources, former NSA voice interceptor Adrienne Kinne.[188]

Coverage of the NSA story subsided substantially for the next year, but in the summer of 2013, further disclosures about the surveillance program once again prompted increased media coverage. On June 5, 2013, *The Guardian* reported that it had obtained a copy of an April 2013 order by the FISC in which the court ordered Verizon to turn over records pertaining to all of the calls in its systems on a daily basis for a three-month period.[189] For students of the NSA story, the revelation was unsurprising: public reports dating back at least to 2006 had confirmed Verizon's cooperation with the NSA's domestic surveillance activities,[190] and the 2013 order provides the government with the same sorts of transactional data that the *Wall Street Journal* highlighted in some of its 2008 reporting on the surveillance program.[191] The new reporting nevertheless confirmed that "[u]nder the terms of the blanket order, the numbers of both parties on a call are handed over, as are location data, call duration, unique identifiers, and the time and duration of all calls."[192] According to *The Guardian*, "[t]he contents of the conversation itself are not covered."[193]

This first new report by *The Guardian* did not reveal

184. Bamford, *NSA Spy Center*, *supra* note 79.
185. *Id.*
186. *Id.*
187. *Id.*
188. *Id.*
189. Greenwald, *NSA collecting phone records*, *supra* note 2.
190. *See, e.g.*, Cauley, *supra* note 81.
191. *See* Gorman, *NSA's Domestic Spying*, *supra* note 79.
192. Greenwald, *NSA collecting phone records*, *supra* note 2.
193. *Id.*

changes to the program beyond what was known before, and it was unable to confirm whether other telecommunication companies have been directed to cooperate under similar orders or whether identical orders were issued on a rolling basis every three months.[194] *The Guardian* article did, however, state that the domestic legal authority for this part of the program came from the "business records" provision of the USA PATRIOT Act, and the report provided strong confirmation that the NSA program has continued on a large scale under the Obama Administration.[195] Indeed, shortly thereafter, *The Guardian* reported on claims by Michael Hayden—NSA Director under President Bush—that the agency's surveillance activities had continued to expand under the Obama Administration.[196]

Within a matter of days, Edward Snowden came forward as the source of the documents underlying *The Guardian's* reporting.[197] A twenty-nine-year-old former contractor who had spent the preceding four years working with the NSA, Snowden claimed to have been disturbed by the breadth of NSA surveillance and motivated by a desire to reveal more information about the program for the benefit of the public.[198] A number of subsequent reports appeared, many focused on Snowden himself,[199] as well as his efforts to seek asylum.[200] As of

194. Greenwald, *NSA collecting phone records*, *supra* note 2. In July, the FISC renewed the Verizon order. Lara Jakes, *FISA Court Approves Continued U.S. Phone Surveillance*, HUFFINGTON POST (July 19, 2013, 6:13 PM), http://www.huffingtonpost.com/2013/07/19/fisa-court-approves-surveillance_n_3625610.html.

195. Greenwald, *NSA collecting phone records*, *supra* note 2.

196. Paul Lewis et al., *US surveillance has 'expanded' under Obama, says Bush's NSA director*, GUARDIAN (June 9, 2013, 1:21 PM), http://www.theguardian.com/world/2013/jun/09/us-surveillance-expanded-obama-hayden.

197. Glenn Greenwald et al., *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, GUARDIAN (June 9, 2013), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

198. *Id.*

199. *See, e.g.*, Barton Gellman et al., *Edward Snowden comes forward as source of NSA leaks*, WASH. POST, June 9, 2013, http://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html; Lana Lam, *Whistle-blower Edward Snowden talks to South China Morning Post*, S. CHINA MORNING POST (June 13, 2013, 8:51 PM), http://www.scmp.com/news/hong-kong/article/1259335/exclusive-whistle-blower-edward-snowden-talks-south-china-morning?page=all; Mark Mazzetti & Michael S. Schmidt, *Ex-Worker at CIA Says He Leaked Data on Surveillance*, N.Y. TIMES (June 9, 2013), http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html?hp&_r=1&.

September 2013, Russia had granted Snowden temporary asylum.[201]

The media also published a number of subsequent stories about the NSA's surveillance activities, many of them based on documents leaked by Snowden. First, *The Guardian* reported on an NSA sub-program called "PRISM."[202] Citing secret, authenticated documents from within the NSA, *The Guardian* reported that PRISM ostensibly allows the NSA to gain direct access to "'emails, chat conversations, voice calls, documents and more . . . from the servers of . . . Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube, [and] Apple.'"[203] All of the companies implicated in the program denied any knowledge that the government had direct access to their servers and insisted that they only turn over information to the government in the face of legitimate, specific requests to do so.[204]

The Guardian subsequently reported that the NSA has paid millions of dollars to the companies involved in PRISM to cover the costs of compliance with the program.[205] The authority for the PRISM program appears to derive from the FAA, under a provision for the deliberate targeting of communications from "foreign nationals believed to be not on U.S. soil."[206] According to *The Guardian*, "Snowden's revelations have shown that US emails and calls are collected in large quantities . . . either deliberately because the individual has been in contact with a foreign intelligence target or inadvertently because the NSA is

---

200. *See, e.g.*, Anna Aruntunyan & Doug Stanglin, *Snowden thanks Russia for asylum, says 'law is winning,'* USA TODAY (Aug. 1, 2013, 4:07 PM), http://www.usatoday.com/story/news/nation/2013/08/01/nsa-edward-snowden-russia-temporary-asylum/2607737/; Michael Pearson et al., *Snowden's asylum options dwindle*, CNN, http://www.cnn.com/2013/07/02/politics/nsa-leak (last updated July 2, 2013).

201. Aruntunyan & Stanglin, *supra* note 200.

202. Dominic Rush & James Ball, *PRISM Scandal: tech giants flatly deny allowing NSA direct access to servers*, GUARDIAN, June 6, 2013, http://www.theguardian.com/world/2013/jun/07/prism-tech-giants-shock-nsa-data-mining.

203. *Id.*

204. *Id.*

205. FISA Amendments Act of 2008, H.R. 6304, 110th Cong. (2008), *available at* https://www.govtrack.us/congress/bills/110/hr6304/text; Ewen MacAskill, *NSA paid millions to cover Prism compliance costs for tech companies*, GUARDIAN (Aug. 22, 2013), http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid.

206. MacAskill, *supra* note 205.

unable to separate out purely domestic communications."[207]

The Guardian also revealed the existence of a sub-program called "Boundless Informant,"[208] which allows the NSA to quantify the data it collects from U.S. computer systems.[209] Boundless Informant appears to focus on transactional data,[210] and the ability of the NSA to discern "how much data [is] gathered from US computers" would seem to contradict some of its public statements.[211]

Further, *The Guardian* reported on the government's interpretation of one of the provisions of the FAA described above—§ 702, which allowed the FISC to issue broad, yearlong warrants for the deliberate gathering of communications where the target of the surveillance is overseas.[212] According to the *Washington Post*, "[t]he law prohibits officials from intentionally targeting data collection efforts at U.S. citizens or anyone in the United States" and "[t]he standards for intentional targeting require that an analyst have a 'reasonable belief,' at least 51 percent confidence, that the target is a foreign national."[213] Yet much turns on the definition of the term "target," and *The Guardian* validated the concerns of FAA critics who thought that incidental collection of American communications would be acceptable under at least one possible interpretation of the relevant statutory provision.[214]

According to the new reports, notwithstanding the overseas targeting requirements, "US communications can still be

---

207. MacAskill, *supra* note 205.

208. Greenwald & MacAskill, *supra* note 1.

209. *Id.*

210. *Id.*

211. Dan Roberts, *White House 'welcomes media interest' in Prism*, GUARDIAN (June 8, 2013, 8:51 PM), http://www.theguardian.com/world/2013/jun/09/prism-security-media-response?guni=Network%20front:network-front%20full-width-1%20bento-box:Bento%20box:Position1:sublinks.

212. FISA Amendments Act of 2008, H.R. 6304, 110th Cong. § 702(a) (2008), *available at* https://www.govtrack.us/congress/bills/110/hr6304/text ("[M]ay authorize . . . for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States . . . .").

213. Robert O'Harrow, Jr. et al., *U.S., company officials: Internet surveillance does not indiscriminately mine data*, WASH. POST, June 8, 2013, http://www.washingtonpost.com/world/national-security/us-company-officials-internet-surveillance-does-not-indiscriminately-mine-data/2013/06/08/5b3bb234-d07d-11e2-9f1a-1a7cdee20287_print.html.

214. *See supra* text accompanying note 151.

collected, retained and used."[215] For example, under guidelines established at least as early as the summer of 2009, the NSA may retain data that could include information on Americans for up to five years, and it could keep and make use of domestic communications that were gathered inadvertently if they "contain usable intelligence, information on criminal activity, threat of harm to people or property, are encrypted, or are believed to contain any information relevant to cybersecurity."[216] Additionally, the article confirmed that in cases "[w]here the NSA has no specific information on a person's location, analysts are free to presume [that person] is overseas."[217] And although targeted surveillance must stop once it becomes known that the target is not overseas, NSA analysts can review the actual content of communications to confirm information suggesting that a target is within the United States.[218] Variations on this last point began to receive additional coverage in the following weeks.

In August of 2013, reports surfaced that the NSA has been searching the contents of "Americans' e-mail and text communications into and out of the country" in search of people who discuss foreigners under surveillance.[219] The process for reviewing such communications involves "temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border."[220] According to an anonymous intelligence official, the process is quick, lasting a few seconds: a computer captures data as they flow from one location to another, reconstitutes the text that those data convey, sorts through the text to find the NSA's chosen terms, and deletes the text that does not contain those terms while saving text that does contain them for subsequent human analysis.[221] The official noted that occasionally, the

215. Greenwald & Ball, *supra* note 2.

216. *Id.*

217. *Id.*

218. *Id.* The process for terminating surveillance of targets later discovered to be within the United States does not exist in cases where the NSA is gathering such large volumes of data that it is not possible to distinguish between U.S. and non-U.S. communications. *Id.*

219. Charlie Savage, *N.S.A. Said to Search Content of Messages to and From U.S.*, N.Y. TIMES, Aug. 8, 2013, http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?_r=0.

220. *Id.*

221. *Id.*

agency would over-collect data, but that the process was monitored and violations were reported.[222]

Within a week, more NSA documents came to light. An internal, May 2012 NSA audit revealed nearly 2,800 "incidents," ranging back over the preceding year, involving the "unauthorized collection, storage, access to or distribution of legally protected communications."[223] Some of these incidents reflected human error, while others reflected computer error, but most appear to have been unintentional.[224] Nevertheless, the total tally (2,776) included only violations recorded in the NSA's Washington, D.C.-area offices.[225] The incidents vary widely in type and significance—examples include violation of a court order, and the improper use of information on 3,000 Americans—but most involve "unauthorized surveillance of Americans or foreign intelligence targets in the United States."[226] (It is impossible to say how many people were affected in total by the incidents.)[227] Further, the rate of violations actually increased during the audit period, despite a substantial rise in the number of personnel dedicated to oversight.[228] Documents also revealed that audit information the NSA provided to oversight bodies differed from the information it produced for the internal audit, with the former omitting some of the incidents included in the latter under narrow interpretations of what information was germane to external oversight.[229]

On August 21, 2013, in response to a Freedom of Information Act (FOIA) lawsuit, intelligence officials declassified an October 2011 FISC opinion in which the court's chief judge castigated the NSA for misleading the FISC as to the nature and scope of some of the NSA's domestic surveillance activities.[230] According to the

---

222. Savage, *supra* note 219.

223. Barton Gellman, *NSA broke privacy rules thousands of times per year, audit finds*, WASH. POST, Aug. 15, 2013, http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html?wpisrc=al_comboPN_p.

224. *Id.*

225. *Id.*

226. *Id.*

227. *Id.*

228. Gellman, *supra* note 223.

229. *Id.*

230. Ellen Nakashima, *NSA gathered thousands of Americans' e-mails before court ordered it to revise its tactics*, WASH. POST, Aug. 21, 2013, http://www.washingtonpost.com/world/national-security/nsa-gathered-thousands-of-americans-e-mailsbefore

opinion, in May of 2011, the NSA revealed to the court that it had been collecting full strings of purely domestic communications that were not from, to, or about a legitimate surveillance target.[231] The NSA had been collecting as many as 56,000 of these communications annually, and the surveillance practices that led to this over-collection had been in place for roughly three years, since the passage of the FAA in 2008.[232] The FISC ordered the NSA to cease such collection, which it deemed unconstitutional, and subsequently approved a modified collection technique in November of 2011.[233] (The modified technique screened purely domestic communications to the FISC's satisfaction, and reduced the retention period for data from five years to two, though further details remain unclear.)[234] The court also criticized the NSA for using improper search terms in digging through the massive amounts of transactional data it obtained about Americans' calling records.[235]

Finally, the *Wall Street Journal* reported on its blog that in several instances NSA officers used the agency's technical capacities to spy on their love interests.[236] The reports did not identify a precise number of such incidents—collectively referred to by the term "LOVEINT"—but they all appear to have involved overseas communications, and most of the incidents were self-reported, resulting in some sort of administrative penalty.[237] Reporting on LOVEINT does not reveal the extent to which these incidents relied on pieces of the NSA's post-9/11 domestic surveillance program.[238]

While these recent revelations have created pressure to reform the NSA program, legislative efforts have thus far been

---

-court-struck-down-program/2013/08/21/146ba4b6-0a90-11e3-b87c-476db8ac34cd_story.html?wpisrc=al_comboPN. The *Washington Post* reported on this issue a week earlier, before the declassification of the FISC opinion. *See* Gellman, *supra* note 223.

231. Nakashima, *supra* note 230.

232. *Id.*

233. *Id.*

234. *Id.*

235. *Id.*

236. Siobhan Gorman, *NSA Officers Spy on Love Interests*, WASH. WIRE (Aug. 23, 2013, 8:45 PM) [hereinafter Gorman, *NSA Love Interests*], http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/.

237. *Id.*

238. *Cf. id.* (going on to report Senator Feinstein's claims that "she's seen no evidence that any of the [LOVEINT] violations involved the use of the NSA's domestic surveillance structure").

unsuccessful.[239] The debate continues, and President Obama has publicly vowed to increase the transparency and oversight of the program,[240] though his proposed changes have yet to have an effect significant enough to modify the analysis that follows.

III. APPLICABILITY OF THE ICCPR TO THE U.S.

Despite copious reporting on the NSA's activities since 9/11, the government has consistently sought to keep details about the program secret, ensuring that even today countless questions remain unanswered. Lacking those answers poses obvious challenges for those seeking to assess the legality of the NSA's operations. If whistleblowers like James Binney are to be believed, the NSA essentially gathers and stores as many communications of Americans—both domestic and international—as it can, focusing its analytical attention on a small subset of those transactions that it deems fruitful. Moreover, according to Binney's account, effectively all of this occurs without any meaningful judicial oversight, or in many cases, any judicial oversight whatsoever. Edward Snowden's leaked documents certainly confirm at least a subset of Binney's allegations. And even operating from facts that have been confirmed by official government sources, the NSA program is clearly a massive undertaking that has repeatedly exceeded the ostensible scope of its domestic legal boundaries, carrying substantial prima facie potential to violate the human right to privacy.

As noted above, Article 17 of the ICCPR protects the human right to privacy.[241] Before examining the terms of that article,

---

239. *See, e.g.*, Jonathan Weisman, *House Defeats Efforts to Rein In N.S.A. Data Gathering*, N.Y. TIMES, July 25, 2013, http://www.nytimes.com/2013/07/25/us/politics/house-defeats-effort-to-rein-in-nsa-data-gathering.html?nl=todaysheadlines&emc=edit_th_20130725&_r=0 (discussing the perceived ambivalence in Congress in the wake of unsuccessful reforms but noting a possible shift).

240. Sabrina Siddiqui, *Obama Proposes FISA Reforms Amid Growing Concerns Over NSA Surveillance*, HUFFINGTON POST (Aug. 9, 2013, 3:12 PM), http://www.huffingtonpost.com/2013/08/09/obama-surveillance-reform_n_3733090.html.

241. It is worth noting that the American Declaration of the Rights and Duties of Man, which has been enforced against the United States by the Inter-American Commission on Human Rights, also offers some protections for privacy. Specifically, Article III states that "[e]very person has the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life." American Declaration of the Rights and Duties of Man, O.A.S. Official Rec., art. III, OEA/Ser.L./V./II.23, doc. 21, rev. 6 (1948), *reprinted in* Basic Documents

however, it is important to address some preliminary matters to ensure the terms on which the ICCPR might apply to the United States. Specifically, this Section will consider the territorial scope of the treaty, the possibility of blanket exemptions from the terms of the treaty, and the United States' use of reservations, understandings, and declarations to modify the applicable terms of the treaty. With respect to the territorial scope of the ICCPR, it will become apparent that the United States takes an unusual and restrictive position. While Section IV will assume that position for the purposes of analyzing the legality of the NSA program, it is important to understand the controversial nature of the United States' view and its implications for the right to privacy.

A. TERRITORIAL SCOPE OF THE ICCPR

One surprisingly complicated issue concerns the scope of the ICCPR as it pertains to the United States. The ICCPR defines its own territorial scope in Article 2(1), which states that "[e]ach State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind . . . ."[242]

There has been some debate about how to interpret "within its territory and subject to its jurisdiction." The Human Rights Committee (HRC)—the committee of experts tasked with monitoring implementation of the ICCPR[243]—interprets the phrase to mean that "a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party."[244] Moreover, the HRC holds the view that the ICCPR extends to non-citizens—including "all

---

Pertaining to Human Rights in the Inter-American System, OEA/Ser.L.V./II.82, doc. 6, rev. 1 at 17. The plain text of this article, however, would seem to set a higher bar than the ICCPR does—prohibiting "abusive attacks" as opposed to "arbitrary or unlawful interference"—and the American Declaration covers fewer countries than the ICCPR. Thus, I have elected to focus attention on the ICCPR.

242. ICCPR, *supra* note 13, art. 2(1).

243. For more information on the Committee, see its website. *Human Rights Committee: Monitoring civil and political rights*, UNITED NATIONS HUMAN RTS., http://www2.ohchr.org/english/bodies/hrc/ (last visited Feb. 3, 2014).

244. U.N. Human Rights Comm., General Comment 31, The Nature of the General Legal Obligations on States Parties to the Covenant, ¶ 10, U.N. Doc. CCPR/C/21/Rev.1/Add. 13 (May 26, 2004).

individuals, regardless of nationality or statelessness, such as asylum seekers, refugees, migrant workers and other persons"—who, for whatever reason, find themselves either within the territory of a state party or within the power or effective control of that state party outside its own territory.[245] The International Court of Justice has taken a similar view, as have prominent commentators like Manfred Nowak.[246]

The United States, rather notoriously, takes a narrower view:

> The United States in its prior appearances before the Committee has articulated the position that article 2(1) would apply only to individuals who were *both* within the territory of a State Party and within that State Party's jurisdiction. The United States is mindful that in General Comment 31 (2004) the Committee presented [a different view]. . . . The United States is also aware of the jurisprudence of the International Court of Justice ('ICJ'), which has found the ICPR "applicable in respect of acts done by a State in the exercise of its jurisdiction outside its own territory," as well as positions taken by other States Parties.[247]

Though the United States appears to be the outlier in taking this interpretation, that fact alone would not necessarily render its view invalid. If it is fair to say that the United States has consistently maintained this position on the scope of the ICCPR, then perhaps as a persistent objector to the more common stance, the United States' view could be taken as applicable—at least for its own obligations under the ICCPR, if not for other parties. Moreover, most of the reporting on the NSA program has focused on its effects for those who are within the United States, so for present purposes, it may not matter a great deal which view is correct.

Nevertheless, the right to privacy (whatever it ultimately entails) illustrates in some of the starkest terms the

---

245. U.N. Human Rights Comm., *supra* note 244.

246. *See* WALTER KÄLIN & JÖRG KÜNZLI, THE LAW OF INTERNATIONAL HUMAN RIGHTS PROTECTION 129-30 (2010) (describing these views); NOWAK, *supra* note 21, at 43-44.

247. PHILIP ALSTON & RYAN GOODMAN, INTERNATIONAL HUMAN RIGHTS 784 (2013) (emphasis added).

counterintuitive implications of the United States' position. In its strongest form, the stance of the United States reduces to the view that the ICCPR permits states to conduct illegal or arbitrary surveillance on anyone outside of their own territory *or* outside of their jurisdiction. Presumably that is indeed the position of the United States, which after all originally established the NSA specifically to conduct foreign surveillance. (Indeed, the agency has since developed an extremely powerful surveillance apparatus that continues to collect substantial information abroad.) But surveillance is particularly troublesome in this respect because much of it can be done from a distance—via satellite, for example, or through the interception of communications that travel through other countries. (By contrast, the United States' reading produces much less counterintuitive results in the case of the right not to be tortured, which governments might have a much harder time violating from afar.)[248]

If one were to generalize the United States' position, then the ICCPR might secure the privacy of Americans *only against arbitrary and illegal intrusion by the United States*, but leave them vulnerable to intrusion by every other government in the world.[249] Similarly, Canadians would be secure as against their own government, but vulnerable to intrusion by all other governments. The same would be true again for people within the territory and jurisdiction of each other state. The right to privacy under the ICCPR would offer very little protection under such a view. Further, it is not obvious that the common, broader reading of the scope of the treaty would be prohibitive for effective intelligence purposes, barring only illegal and arbitrary interference with privacy.[250]

Whatever the geographic scope of the treaty, each state must do more than simply abstain from intruding on the privacy rights of those within its territory and jurisdiction. The general rule is that states must respect, protect, and fulfill the rights of those who fall within the scope of a binding treaty.[251] But without a

248. Put another way, it is difficult to conceive of a state directly violating many rights, such as the right not to be tortured, without having some control over the person whose rights are being violated. Privacy is different in this respect.

249. *See* ICCPR, *supra* note 13, art. 17(1).

250. We will consider the meaning of the provisions of Article 17 in more detail below.

251. *See What are human rights?*, UNITED NATIONS HUMAN RTS.,

duty on states not to engage in broad surveillance of those outside their territory or jurisdiction, the responsibility of each state to *protect* its own subjects from the prying of dozens of other states would be impossible to meet. To the extent that states literally could not protect their own from violations by other countries—violations that on the United States' view would not actually contravene the treaty—the number of privacy intrusions that the ICCPR would countenance is extraordinary, potentially defeating the object and purpose of the treaty as concerns the right to privacy.[252] If even a subset of the rights guaranteed in the ICCPR cannot be protected in any meaningful way as a result of a particular reading of the treaty, then that reading is almost certainly inadequate. Nevertheless, if only to yield more persuasive results, the analysis that follows will stipulate to interpreting the human rights implications of the NSA program under the United States' own position on the reach of the ICCPR.

B. BLANKET EXEMPTIONS FROM THE ICCPR

Another preliminary matter to consider is whether there is reason to think that the ICCPR would be entirely inapplicable to the NSA program. The answer here appears to be negative. For one, "[w]ith respect to the application of the Covenant and [IHL], the United States has not taken the position that the Covenant does not apply 'in time of war.'"[253] By foreclosing the possibility that the ICCPR is simply inapplicable due to wartime considerations, there is no other obvious reason to think that the ICCPR would be inapplicable, especially (given the United States' position on territorial scope) within the United States.[254]

---

http://www.ohchr.org/EN/Issues/Pages/WhatareHumanRights.aspx (last visited Feb. 3, 2014); *see also Human Rights: The Human Rights-Based Approach*, UNITED NATIONS POPULATION FUND, http://www.unfpa.org/rights/approaches.htm (last visited Feb. 3, 2014) (expressing this commonplace maxim).

252. One possible response might be to note that the United States position is not, in fact, universal. But the position of the United States is based on a textual reading of the treaty, suggesting that other states could in principle take the same stance, thereby opening up that stance to critical assessment for compatibility with the treaty's object and purpose. Moreover, the U.S. has so much power to conduct surveillance abroad that even if it alone took this particular reading, the result could be a substantial number of acts that run contrary to the spirit of the ICCPR. In any event, as a somewhat separate matter, it is worth noting that states taking a broader reading of the reach of the ICCPR may need to consider whether their foreign intelligence surveillance activities align with their treaty obligations not to interfere arbitrarily or illegally with various protected privacy interests.

253. ALSTON & GOODMAN, *supra* note 247, at 784.

254. *See supra* Section III(A).

Further, while Article 17 admits of derogation "in time[s] of public emergency,"[255] to derogate from any eligible article of the ICCPR, the United States must "immediately inform other States Parties [to the ICCPR], through the intermediary of the Secretary-General . . . of the provisions from which it has derogated and of the reasons by which [the derogation] was actuated [, as well as, subsequently, send another communication] on the date on which it terminates such derogation."[256] The United States has not taken any of these steps, so it cannot have derogated from the requirements of Article 17.

C. RESERVATIONS, UNDERSTANDINGS, AND DECLARATIONS

The final preliminary matter is whether the United States has posited reservations, understandings, or declarations (RUDs) with respect to the meaning of the terms of Article 17.[257] If it had, those would shape our analysis; however, the United States did not attach any such modifications when it ratified the ICCPR in 1992, except to say that Article 17 (among many others) is not self-executing, thereby keeping it from being judicially enforceable until and unless the United States passes relevant domestic legislation.[258] That position may have implications for the practical efficacy of arguments under the ICCPR, especially as concerns domestic litigation, but it does not affect the underlying legal analysis involved in making such arguments. Thus, Article 17 of the ICCPR appears to be in full effect for purposes of analyzing the implication of the NSA program on the rights of people within the United States.

---

255. *See* ICCPR, *supra* note 13, arts. 4(1)-(2) (offering this quote, and omitting Article 17 from the list of non-derogable provisions).

256. *Id.* art. 4(3).

257. For some background on RUDs, see generally Eric Neumayer, *Qualified Ratification: Explaining Reservations to International Human Rights Treaties*, 36 J. LEGAL STUD. 397 (2007).

258. *See International Covenant on Civil and Political Rights*, UNITED NATIONS TREATY COLLECTION, http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en#EndDec (last visited Feb. 3, 2014) (listing the United States' RUDs on the ICCPR, which includes no references to Article 17 specifically and only contains one relevant declaration to the effect that Article 17 is not self-executing).

IV. THE RELEVANCE OF ARTICLE 17 FOR THE NSA PROGRAM

Recall the text of Article 17: Article 17(1) states that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation,"[259] while Article 17(2) adds that "[e]veryone has the right to protection of the law against such interference or attacks."[260] It may be worthwhile to gain some perspective on the right to privacy in general before assessing its more specific terms (barring arbitrary or unlawful interference) and its precise applications to the NSA program.

A. OVERVIEW

Fernando Volio argues that the right to privacy is one of the most important rights protected in the ICCPR, especially to the extent that it protects "individual personality."[261] He points out that the ICCPR uses different constructions to begin its various articles, such as "all peoples," "everyone," "all citizens," and so on; however, Article 17 begins with a stronger construction: "No one shall be deprived . . . ."[262] According to Volio, the phrase "'[n]o one' appears whenever the Covenant seeks to underscore a basic freedom which may not be denied to any person."[263] Moreover, Volio points out that "no limitation provision was added and the rights are protected without qualification."[264]

Manfred Nowak highlights the same textual point: "Art[icle] 17 does not contain a limitation clause allowing for restrictions in the interest of public order or similar purposes."[265] According to Nowak, however, the reason for the omission appears to be that states did not want to have excessive restrictions on their latitude to determine the limitations on the provisions of Article 17.[266] At the same time, Nowak observes that there was little controversy

259. *See* ICCPR, *supra* note 13, art. 17(1).

260. *Id.* art. 17(2).

261. Fernando Volio, *Legal Personality, Privacy, and the Family*, *in* THE INTERNATIONAL BILL OF RIGHTS: THE COVENANT ON CIVIL AND POLITICAL RIGHTS 185, 186 (Louis Henkin ed., 1981).

262. *Id.* at 190.

263. *Id.*

264. *Id.* at 192.

265. NOWAK, *supra* note 21, at 381.

266. *Id.* (noting that amendments which would have listed limitations were voted down in part due to the desire of states to construct their own limitations).

about adopting a general protection for the right to privacy in the ICCPR because of the inclusion of a similar right in the Universal Declaration of Human Rights (UDHR).[267]

Nowak also emphasizes that "disregard for personal data and secret surveillance measures by private security companies [] led during the drafting of Art[icle] 17 to a certain emphasis on the *positive obligation of the States to protect privacy* against interference and attacks from others."[268] While Nowak notes that several states, including the United States, United Kingdom, and Australia, took the view during treaty negotiations that the article only offered protection against interference by the state (lest states had to make changes to their private law systems), he also points out that the view of these states did not win out.[269]

The commentary on and jurisprudence of the European Court of Human Rights (ECtHR) may also be helpful in shaping our interpretation of the ICCPR. Article 8 of the European Convention on Human Rights (European Convention)[270] strongly resembles Article 17 of the ICCPR, reading as follows:

> 8(1): Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 8(2) There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[271]

The European Convention's language is less strict than the language of the ICCPR, especially insofar as its qualifying Article, 8(2), explicitly admits of numerous exceptions not listed

---

267. *See* NOWAK, *supra* note 21, at 385 (implying this).

268. *Id.* at 379 (emphasis in original).

269. *Id.* at 379-80.

270. For some targeted analysis of how the European Convention on Human Rights might handle mass surveillance, see Memorandum from Mr. Pieter Omtzigt, Rapporteur, Comm. on Legal Affairs & Human Rights (Jan. 23, 2014), *available at* http://website-pace.net/documents/19838/419003/AS-JUR-2014-02-EN.pdf/2c9ba3c3-d456-4471-a39d-087987ef1208.

271. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221, Europ. T.S. No. 5 [hereinafter European Convention].

in the ICCPR's corresponding Article, 17(2). On the other hand, some commentators have found Article 8(2) to provide better protection than Article 17 because the former is less vague.[272] The exclusion of an exhaustive list of limitations on the right to privacy in the ICCPR followed in part from a concern by states that such a list would actually make it more difficult for them to interfere with the right to privacy.[273] But it is worth noting that some states objected to a list styled on Article 8(2) of the European Convention for its implication that the limitations on interference would apply only to state actors (and not also to private parties).[274] There is also a question as to the difference between the European Convention's demand of "respect for" the interests in Article 8 as against the ICCPR's prohibition of the "interference with" the interests in Article 17. The ECtHR has read the "respect for" language as entailing positive (not merely negative) obligations.[275] But then again, the widely accepted "respect, protect, fulfill" framework for the ICCPR would seem to entail positive obligations for states as well, notwithstanding the negative language of Article 17.[276]

Additionally, beyond their syntactical differences, the terminology in the two articles is somewhat different. The European Convention protects *private life*, *family life*, home, and correspondence,[277] while the ICCPR protects *privacy*, *family*, home, and correspondence.[278] To the extent that reviewing the ECtHR approach to the right to privacy is merely instructive and not decisive, we may infer that the semantic similarities here are by design, and we may treat each of the four interests in the ICCPR's Article 17 as analogous to the four interests in the European Convention's Article 8. (Nowak himself explicitly indicates that "privacy" in the ICCPR and "private life" in the European Convention "mean basically the same thing.")[279] The absence of clear, defining boundaries for these four interests in

---

272. NOWAK, *supra* note 21, at 381 (noting that some scholars take this view).

273. *Id.*

274. *Id.*

275. *See* D.J. HARRIS, M. O'BOYLE, & COLIN WARBRICK, LAW OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 321 (1995) (describing these developments).

276. *See, e.g.*, KÄLIN & KÜNZLI, *supra* note 246, at 129 (discussing the duty to guarantee these rights); *see also* NOWAK, *supra* note 21, at 379 (reaffirming positive obligations under Article 17).

277. *See* European Convention, *supra* note 271, art. 8(1).

278. *See* ICCPR, *supra* note 13, art. 17(1).

279. NOWAK, *supra* note 21, at 385.

the ECtHR system allows for them to overlap, providing the court with flexible coverage for matters that are difficult to classify precisely.[280]

Note that the ECtHR is more forgiving of government interference with the right to privacy when the stated purpose for the interference is the protection of national security (rather than, say, the pursuit of standard criminal prosecutions).[281] In the context of wiretapping, the ECtHR largely defers if there exist "formal legality and procedural guarantees."[282] Moreover, "[w]here the authorities have been able to point to a lawful basis for wire-tapping and procedural protections which satisfy the [requirement of access to a remedy], the institutions have never disputed that the interception was 'necessary in a democratic society.'"[283] Yet the ECtHR has also acknowledged the threat posed by "secret surveillance measures[] 'of undermining or even destroying democracy on the ground of defending it, [and] affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.'"[284] To the extent we wish to draw inferences from relevant outcomes in the ECtHR, this is surely relevant, so we will return to it below.

Because Article 17 of the ICCPR does not offer an explicit exception for national security concerns (or for any other reason), Volio is skeptical of the possibility of justified interference with the right to privacy.[285] Nowak takes a less stringent view, noting that although Article 17 does not explicitly admit of exceptions, assessing interference that is both lawful and non-arbitrary "requires a precise balancing of the circumstances in a given case, paying regard to the principle of *proportionality*."[286] He claims that to inform our analysis of which purposes might justify interference with the right to privacy under the ICCPR, we need to look at limitation clauses from Articles 12, 18, 19, 21, and 22 of

280. HARRIS, O'BOYLE, & WARBRICK, *supra* note 275, at 303.

281. *See id.* at 346 (elaborating further, specifically by citing cases to this effect).

282. *Id.* at 354.

283. *Id.* at 354-55.

284. *Protection of Personal Data*, EUR. CT. OF HUM. RTS. 1 (July 2013), http://www.echr.coe.int/Documents/FS_Data_ENG.pdf (quoting Klass v. Germany, App. No. 5029/71, 28 Eur. Ct. H.R. (ser. A) ¶ 49 (1978)).

285. *See* Volio, *supra* note 261, at 192 (claiming the rights in Article 17 "are protected without qualification").

286. NOWAK, *supra* note 21, at 383 (emphasis in original).

the ICCPR—as well as, potentially, the limitations from Article 8(2) of the European Convention.[287] But as a rule of thumb, he suggests the following:

> In evaluating whether interference with privacy by a State enforcement organ represents a violation of Art[icle] 17, it must especially be reviewed whether, in addition to conformity with national law, the specific act of enforcement had a purpose that seems legitimate on the basis of the Covenant in its entirety, whether it was predictable in the sense of rule of law and, in particular, whether it was reasonable (proportional) in relation to the purpose to be achieved.[288]

Nowak's position seems to echo the view of the Human Rights Committee, which states that "[i]nterference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims[,] and objectives of the Covenant."[289] The Committee also observes that "[t]he introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims[,] and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances."[290]

In light of the foregoing, Volio's position appears to be implausibly strong. Nowak's description of the debate around the passage of Article 17 suggests that states accepted the existence of reasons that might justify interfering with the right to privacy, even if no explicit list of limitations appears in the Article itself.[291] Indeed, Nowak points to several other articles in the ICCPR to inform our understanding of what sorts of reasons might justify interference with the right to privacy, and all of those articles list national security, public safety, or both among

---

287. NOWAK, *supra* note 21, at 383.

288. *Id.*

289. U.N. Human Rights Comm., General Comment 16, The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Article 17), ¶ 3, U.N. Doc. HRI/GEN/1 Rev. 6 (Apr. 8, 1988) [hereinafter General Comment 16], *available at* http://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=453883f922.

290. *Id.* ¶ 4.

291. NOWAK, *supra* note 21, at 381 (describing the rejection of amendments that would have enumerated such justifications due in part to a desire to allow states some flexibility in defining the appropriate justifications).

factors that can limit the relevant rights.[292] Thus, we can stipulate for the purposes of this Article's analysis that legitimate concerns about national security (or public safety) would give the United States a reason to justify its interference with the right to privacy.

The main question that remains is whether national security concerns can justify interference with the right to privacy *even if that interference is unlawful or arbitrary*. A plain reading of the text of Article 17 might imply an affirmative answer, for the right protected there is, specifically, freedom from unlawful and arbitrary interference with one's privacy, correspondence, and so on. Thus, an exception to those protections would seem to be an exception to the prohibition of unlawful and arbitrary interference—not an exception to the prohibition of interference per se. Clearly, the most favorable position to the United States would be that national security justifies unlawful or arbitrary interference with the right to privacy.

Yet "unlawful" and "arbitrary"—as discussed in more detail below—are particularly egregious forms of interference, such that it would seem strange to admit of broad exceptions to their prohibition. Moreover, even legitimate national security concerns do not obviously require that a state have the authority to engage in unlawful or arbitrary interference with any interest, let alone a privacy interest (as opposed to lawful, non-arbitrary interference).[293] Both the Human Rights Committee and Nowak suggest that lawfulness and non-arbitrariness are necessary conditions for *justifiable* interference—that is, that a state party could only justify lawful, non-arbitrary interference—and that such a state can only interfere with privacy in a manner proportionate to the pursuit of a legitimate aim (perhaps like national security).[294] Additionally, a similar analysis appears to

---

292. NOWAK, *supra* note 21, at 381; *see also* ICCPR, *supra* note 13, arts. 12, 18, 19, 21, 22 (each listing one or both of these reasons for limiting the rights they respectively protect).

293. In other words, given the power that states have to shape their own domestic laws, and the questions about the value of pursuing any policy arbitrarily, even states protecting their own national security do not seem to require the latitude to violate protected interests either unlawfully or arbitrarily.

294. *See supra* text accompanying notes 286-290; *see also* Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development*, U.N. Human Rights Council, ¶ 28, U.N. Doc. A/HRC/23/40, 8 (Apr. 17, 2013) (by Frank La Rue) [hereinafter Special

prevail in the case of the European Convention, where lawfulness remains a necessary condition for interference with the right to privacy (though it may be worth noting that lawfulness is built into the exceptions clause of Article 8(2) of the European Convention).[295]

We will explore the content of the specific prohibitions on arbitrary and unlawful interference below, once we have reviewed the relevant protection of the interests enumerated in Article 17. For now, we may accept that there could be reasons for interfering with privacy under the ICCPR. We can also conclude that lawful and non-arbitrary interference is not permitted simply because it is lawful and non-arbitrary; rather, the state must avoid unlawful and arbitrary interference generally, and it can only interfere with the right in a lawful, non-arbitrary manner if it can justify doing so based on proportional action designed to advance certain types of state interests, presumably including national security.

B. THE SCOPE OF THE TERM "PRIVACY"

What interests fall within the right to privacy? Volio argues that the right "includes much besides the private matters explicitly listed"—namely, family, home, correspondence, honor, and reputation.[296] He claims that the term "privacy" carries its own substantial content that extends beyond the itemized list in Article 17 (pointing to lists of subcomponents of the right to privacy identified by the 1967 Nordic Conference and Dean Prosser's list of factors for defining privacy under American tort law).[297]

Nowak claims that privacy, as protected in the ICCPR, comprises "[t]hat sphere of *individual autonomy* whose existence

---

Rapporteur Report], *available at* http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf ("The framework of article 17 of the ICCPR enables necessary, legitimate and proportionate restrictions to the right to privacy by means of permissible limitations.").

295. *See* RICHARD CLAYTON & HUGH TOMLINSON, THE LAW OF HUMAN RIGHTS § 12.237 (2009) (noting this point).

296. Volio, *supra* note 261, at 192-93.

297. *See id.* at 192-95 (undertaking this assessment). Volio also makes some more specific observations as well. He highlights the Human Rights Committee's expression of concern about how states protect individuals from databanks and from surveillance by state intelligence agencies, and he notes the Committee's suggestion that individuals might need to be informed when under surveillance. *Id.* at 196.

and field of action does not touch upon the sphere of liberty of others . . . ."[298] He notes that "[i]n the 20th century, [protection for the home, family and correspondence] . . . were joined by secrecy of telecommunications, by the general protection of personal data and the genetic code of human beings."[299] Like Volio, Nowak also lists several components of a right to privacy that reach beyond the enumerated categories in Article 17 but that are protected under the broader term "privacy."[300] He identifies relevant interests that fall under headings such as identity, integrity, intimacy, autonomy, communication, and sexuality.[301]

Of particular relevance for present purposes is the category of intimacy, which Nowak claims includes the "protection of personal data."[302] Nowak claims that such protection is especially important because of "technological developments in electronic data processing."[303] Under Article 17(2), state parties must "regulate the recording, processing, use and conveyance of automated personal data and . . . protect those affected against misuse by State organs as well as private parties."[304] Moreover, "[i]n addition to prohibiting data processing for purposes that are incompatible with the Covenant, data protection laws must establish rights to information, correction and, if need be, deletion of data and to provide effective supervisory measures."[305]

Academic commentators are not alone in holding these views. The Human Rights Committee has also spoken directly about the collection and storage of personal data:

> In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public

298. NOWAK, *supra* note 21, at 378 (emphasis in original).

299. *Id.*

300. *See id.* at 385-92 (discussing the coverage provided by the word "privacy.")

301. *Id.*

302. *Id.* at 388. While "communication" would seem relevant for us as well, it turns out to be reasonably uncontroversial that most of the communications that are subject to interception by the NSA fall into an explicit term in Article 17—namely, "correspondence." We will revisit this point below.

303. NOWAK, *supra* note 21, at 388.

304. *Id.*

305. *Id.*

> authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[306]

The ECtHR also seems to assume that wiretapping interferes with the target's private life (independently of whether it interferes with correspondence).[307] Moreover, once the state has collected information, for the ECtHR there is a further question about how it retains or uses that information.[308] Indeed, "[m]ere storage of information about an individual's private life amounts to interference within the meaning of Article 8 [of the European Convention]."[309] And as concerns covert government surveillance, while such activity can be justified under certain conditions in the ECtHR system, the court requires adequate safeguards.[310]

---

306. General Comment 16, *supra* note 289, ¶10.

307. *See* HARRIS, O'BOYLE, & WARBRICK, *supra* note 275, at 309 (defending this view). For more on the ECtHR stance toward wiretapping see *Protection of Personal Data*, *supra* note 284, at 3 (summarizing relevant precedents, which include several findings of article 8 violations grounded in wiretapping).

308. HARRIS, O'BOYLE, & WARBRICK, *supra* note 275, at 310-11; *see also Protection of Personal Data*, *supra* note 284, at 5-7 (summarizing relevant precedents on the collection and use of personal data).

309. *Protection of Personal Data*, *supra* note 284, at 1.

310. *Id.* The court has not been particularly specific about what safeguards might be adequate. For example, in *Klass v. Germany*, it articulated a fluid standard for adequacy of privacy protections for covert government surveillance. "The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law." Klass v. Germany, App. No. 5029/71, 28 Eur. Ct. H.R. (ser. A) ¶ 50 (1978), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510#. In *Rotaru v. Romania*, the court observed that Article 8 of the Convention requires

> safeguards established by law which apply to the supervision of the relevant services' activities. Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, *inter alia*, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure.

Rotaru v. Romania, App. No. 28341/95, 8 Eur. Ct. H.R. 449 ¶ 59, *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58586#{"itemid":["001-58

Moreover, the ECtHR would seem to concur with the Human Rights Committee and with Nowak on the problems with collecting vast amounts of transactional data. Under the approach of the ECtHR, respect for one's "private life" appears implicated by the nonconsensual collection of personal information by state officials.[311] This includes such information as is gathered by a census and as one might surrender in being fingerprinted and photographed by the police.[312] It can also include information "relating to [a person] through [his or] her use of the telephone, e-mail and [I]nternet."[313] If we can infer anything from the conclusions of the ECtHR, surely a detailed history of one's financial transactions, the recipients of one's correspondence, and the subjects of one's emails would be problematic as well.[314]

Additionally, for the ECtHR, the mere possibility that a state might use a criminal statute to prosecute an individual for private behavior (for instance, intimate same-sex relations) could be sufficient to violate the right to privacy of a person who forms such relations—even if the state never ultimately charges the person in question.[315] The psychological effect of the uncertainty in those circumstances is sufficient to interfere with the freedom to engage in private behavior.[316] Indeed, that principle has a

---

586"]}. Even more recently, in *Association "21 December 1989" and Others v. Romania*, the court found a violation of Article 8 when secret services undertook surveillance of an applicant and the relevant "domestic law did not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities." Press Release, European Court of Human Rights, Crackdown on Romanian Demonstrations in 1989: Lack of Effective Investigation and Use of Secret Surveillance 5 (May 24, 2011), *available at* http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx?i=003-3549731-4011007#{"itemid":["003-3549731-4011007"]}.

311. HARRIS, O'BOYLE, & WARBRICK, *supra* note 275, at 309.

312. *Id.*

313. *See Protection of Personal Data*, *supra* note 284, at 8 (attributing the court's finding of an Article 8 violation in *Copland v. United Kingdom* to the "collection and storage" of that same information about the applicant).

314. The last of these might simply fall into the category of correspondence, as discussed below.

315. HARRIS, O'BOYLE, & WARBRICK, *supra* note 275, at 336. More specifically, in *Dudgeon v. United Kingdom*, the court held that the mere possibility of prosecution under a law criminalizing homosexual relations "continuously and directly affects [the petitioner's] private life." Dudgeon v. United Kingdom, App. No. 7525/76, 45 Eur. Ct. H.R. (ser. A) ¶ 41 (1981), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57473#.

316. *Dudgeon*, 45 Eur. Ct. H.R. ¶¶ 40-41 (accepting the applicant's claims to

broader application: a recurring theme in ECtHR jurisprudence on privacy is that states violate the European Convention when undertaking various surveillance activities without first establishing "sufficient clarity" as to the permissible "scope and manner" of those activities.[317] Applicants are thus well positioned if they can show why they might be the target of surveillance, even if they in fact turn out not to have been, for "'[i]n the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance.'"[318]

C. THE SCOPE OF THE TERM "CORRESPONDENCE"

Traditional definitions of the term "correspondence" refer specifically to letters,[319] but that definition does not stand for legal purposes under the ICCPR. Nowak notes that the term "correspondence" "primarily means written letters, [but] today covers all forms of communications over distance, i.e., by telephone, telegram, telex, telefax, e-mail and other mechanical or electronic means of communication."[320] Similarly, Volio writes that "[c]orrespondence clearly includes written communication . . . [as well as] direct oral communication, and today must include communication by any mechanical or electronic means."[321] Both the Human Rights Committee[322] and the ECtHR have also classified phone calls as falling within the category of correspondence.[323]

In Nowak's view, under Article 17(2), state parties have a "comprehensive obligation . . . to ensure that letters, telegrams,

---

suffering "fear and distress," and going on to find the existence of the law causing those feelings as constituting an interference with the right to privacy).

317. *See Protection of Personal Data*, *supra* note 284, at 2, 4 (noting *Wisse v. France*, *Kruslin v. France*, and *Vetter v. France* as examples of cases where states were found to be in violation of Article 8 because their domestic laws do not indicate "with sufficient clarity . . . the scope or manner" of permissible activity).

318. HARRIS, O'BOYLE, & WARBRICK, *supra* note 275, at 337 (internal citation omitted).

319. *See, e.g.*, THE AMERICAN HERITAGE DICTIONARY 327 (2d college ed. 1982) (defining "correspondence" as "[c]ommunication by the exchange of letters").

320. NOWAK, *supra* note 21, at 401.

321. Volio, *supra* note 261, at 197.

322. U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, Third Periodic Report (Bulgaria)*, ¶ 22, U.N. Doc. CCPR/C/BGR/CO/3 (Aug. 19, 2011).

323. HARRIS, O'BOYLE, & WARBRICK, *supra* note 275 at 303 n.7, 320.

emails, etc. are actually delivered to the desired recipient and are not inspected by third parties."[324] For Nowak, this means that "[e]very withholding, censorship, inspection of (or listening to) or publication of private correspondence represents *interference* within the meaning of Art[icle] 17."[325] Again, Volio has a similar take: the nature of the protections for correspondence includes protection "primarily against divulgence to anyone other than the intended recipient," but also protection "against interruption or other interference" such as would delay or prevent its delivery.[326]

Nowak makes some more specific claims that are relevant as well, pointing out that state surveillance for counterterrorism or criminal prosecution amounts to the most common type of interference with correspondence.[327] He emphasizes that, "[s]imilar to house searches, such interference is permissible only on the basis of a specific decision by a State authority expressly empowered by law to do so (usually a court) for the purpose of securing evidence or preventing crime and must respect the principle of proportionality."[328] Here again the jurisprudence of the ECtHR is instructive. In *Campbell v. UK*, the ECtHR found that a prison regime that permits the officials to open and read letters sent by inmates supplied one such inmate with a colorable claim to a violation of his Article 8 right to privacy, even if he could not show that his own letters had, in fact, been compromised.[329]

In sum, the collection and review of verbal communications, whether oral or written, would seem to amount to interference with correspondence under Article 17. Inferring from the ECtHR system, even the mere threat that such correspondence could be reviewed may be sufficient to ground a complaint of interference with correspondence.[330]

---

324. NOWAK, *supra* note 21, at 401. Note that this does not mean there is a right to a perfectly functioning postal service. *Id.*

325. *Id.* (emphasis in original).

326. Volio, *supra* note 261, at 197.

327. NOWAK, *supra* note 21, at 402.

328. *Id.*

329. HARRIS, O'BOYLE, & WARBRICK, *supra* note 275, at 335. This approach quite plainly diverges for the recent Supreme Court decision in *Clapper v. Amnesty International, USA*, which we will discuss briefly below. For more on how the ECtHR has interpreted the application of Article 8 to the correspondence of persons detained by the state see *Protection of Personal Data*, *supra* note 284, at 2.

330. *See Protection of Personal Data*, *supra* note 284, at 1 ("Mere storage of information about an individual's private life amounts to interference within the

D. TAKING STOCK

The preceding analysis of the right to privacy under Article 17 of the ICCPR is not exhaustive. It has discussed neither protection of the family, nor protection of the home—let alone honor, reputation, or other areas of coverage arguably falling within the ambit of the broader term "privacy."[331] The areas covered, however, are those most relevant to analysis of the implications of the NSA surveillance program. Reports on the NSA program have thus far revealed three major ways in which the United States government is potentially infringing the right to privacy under the ICCPR:[332] first, through the collection or inspection of emails; second, through the recording or analysis of phone calls; and third, by storing or reviewing transactional data. The first two of these fall within the scope of protections for correspondence, while the third falls (by and large) under the protection for privacy more generally.

Actual review of any of these forms of information unequivocally constitutes interference,[333] and states have a positive obligation to prevent the review of private information (like the content of communications) by third parties[334]—an obligation undermined by the collection and retention of that information. Moreover, if ECtHR jurisprudence is instructive here, both the simple collection of these forms of information[335] and the fact that the government can review them may be sufficient to produce an intrusion.[336] Thus, all three of these forms of data-gathering or review appear to constitute "interference" under Article 17(1).

Focusing on these three areas, even if limited to those individuals who are within the territory and subject to the jurisdiction of the United States, the NSA program carries the potential for a large number of violations of the right to privacy

---

meaning of Article 8 (right to respect for private life) of the European Convention on Human Rights.").

331. *See supra* Section IV(B).

332. Of course, it is possible that the NSA is gathering yet further information in other ways that would introduce new categories into our analysis were we to learn of it.

333. *See supra* text accompanying note 325.

334. *See supra* text accompanying note 324.

335. *See supra* text accompanying notes 309-11.

336. *See supra* text accompanying notes 307-318, 329.

under Article 17 of the ICCPR. The question remains whether such collection can be justified under the terms of the ICCPR—whether it is lawful, non-arbitrary, and proportionate.

Before proceeding to unpack the ways in which the ICCPR could apply to the NSA program, it is helpful to consider certain peculiarities about the right to privacy as discerned by the preceding analysis. As indicated above, the Human Rights Committee, various commentators, and the ECtHR all suggest that even the improper interception of correspondence or data, without review, can be enough to violate the right to privacy. Yet the harm caused by the wrongful *collection* of data or correspondence seems to differ from the harm caused by the wrongful *review* of data or correspondence. To the extent that much of the public reporting about the NSA program contains allegations specifically about the broad collection of information,[337] a substantial proportion of the concern about the program (though certainly not all of it) tracks the former more than the latter. Those who dispute the concerns about mere collection of information may find that share of worry about the program overblown.[338]

The fact that the government has certain information on hand—even if analysts never review it—leaves the subjects of that information vulnerable and uncertain. This is especially the case where it remains unclear what information is available to the government, as well as if and when the information will be accessed. The theoretical possibility of improper access to stored information (against whatever safeguards the state imposes) can be enough to trigger genuine worries even where there is supposed to be less uncertainty. That is essentially the harm that the ECtHR has identified in *Dudgeon v. United Kingdom*,[339]

---

337. *See, e.g.*, Gorman, *NSA's Domestic Spying*, *supra* note 79; Greenwald, *NSA collecting phone records*, *supra* note 2.

338. *See, e.g.*, Richard A. Posner, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html (arguing that while "collection . . . of personal data is said to invade privacy[, . . .] machine collection and processing of data cannot, as such, invade privacy"); Richard A. Epstein, *In Defense of the NSA*, DEFINING IDEAS (June 18, 2013), http://www.hoover.org/publications/defining-ideas/article/149766 (asserting that there is a "line between collection and use [of information collected by the NSA]").

339. *See* Dudgeon v. United Kingdom, App. No. 7525/76, 45 Eur. Ct. H.R. (ser. A) ¶¶ 40-41 (1981) (noting the "fear and distress . . . suffered in consequence of the existence of the laws . . .").

and it is difficult to dispute.

Perhaps some will find it worse for the government to review private information or correspondence, as those acts would clearly amount to violations of privacy in fact, whereas simple collection of information might seem like a precursor or threat to the violation of privacy. Alternatively, one might see the mere possession of private information by an unauthorized party to be a direct affront to privacy.[340] However one cognizes the relevant harms, the link between the two is clear enough, as are the interpretations of the ICCPR and European Convention.[341] Both fall, defensibly, within the bounds of the human right to privacy.

A further complication that arises with respect to the collection of emails (and perhaps certain information available online) is that companies providing email services often have privacy policies that explicitly allow them to collect certain information.[342] Google's privacy policy, for example, lists several sorts of information that it gathers in connection with the use of its services, including Internet search histories and, in some cases, GPS tracking information.[343] There is no doubt that using email providers like Google involves granting a third party access to a substantial amount of personal information, raising the following question: to what extent does consenting to such collection undermine the ability of individuals to claim that the government is violating their privacy rights by gathering much of the same information?[344]

Whatever the ultimate answer to that question, there are plainly significant differences between consensual data collection by private companies in exchange for the use of their services and nonconsensual,[345] wholesale collection of data by a government

340. For much more nuanced discussions of the different harms posed by collection and review of private information, see generally Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. R. 1934 (2013) and Daniel J. Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. R. 745 (2007).

341. *See supra* text accompanying notes 333-336 (noting the interpretations of the ICCPR and European Convention that would condemn mere collection of information).

342. *See, e.g., Policies & Principles: Privacy Policy*, GOOGLE, http://www.google.com/intl/en/policies/privacy/ (last modified Dec. 20, 2013) (outlining the information Google gathers from users of its services).

343. *Id.*

344. I am grateful to Faiza Patel for raising this question.

345. For example, Google's stated policy is not to turn over any information to the

that has coercive power over the subjects of those data. Moreover, given the necessity of conducting certain business online, people are often effectively forced into using technology that makes it easier for the private companies to gather information of the sort Google describes in its policy. Employees are often required to use company email to perform their duties, and students at colleges and universities (not to mention some secondary schools) literally must use their email to some extent to remain apprised of academic developments. If it turns out that email providers have truly deficient privacy policies under conditions where individuals have effectively no choice but to consent, it is not so clear that the policies are valid. Perhaps these agreements are more like contracts of adhesion.

Finally, consenting to the terms of use for an email account is certainly not the same thing as consenting to the active harvesting of one's email communications—outside the terms of the account provider's privacy policy—by the government. To the extent that the government picks up emails via splitter cabinets, or copies and searches the text before deleting the emails, this is very much an applicable consideration in the context of the NSA program.[346]

---

government unless compelled by law. *Policies & Principles: Privacy Policy*, *supra* note 342. Additionally, it can be difficult or impossible even for experts, let alone laypeople, to figure out when their information will be at risk of submission to the government under valid legal requests.

346. This summary is necessarily cursory, simply laying out a few reasons why we may continue with our analysis. For more detailed discussions and diverse perspectives, see generally Jonathan Bick, *Internet Communications Privacy Rights: Existing Statutes and Case Law Reduce Constitutional Protections*, 195 N.J. L. J. 793 (2009), *available at* http://www.bicklaw.com/internetcommunicationprivacy rights.htm (summarizing some domestic legal standards for expectations of privacy); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007) (canvassing four models of protection for privacy under the Fourth Amendment, and advocating the use of all of them depending on which is most appropriate in a given context); Lior Strahilevitz, *A Social Networks Theory of Privacy* (U. Chicago Public Law Working Paper No. 79 Dec. 2004), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=629283 (arguing that courts should use objective metrics such as the likelihood that certain information will become known to the public, rather than subjective expectations of privacy, in deciding which information about a person is legally protected); Joshua Foust, *Nine Dashed-Off Points on the NSA "Scandal,"* JOSHUA FOUST: RECOVERING JOURNALIST (June 5, 2013), http://joshuafoust.com/nine-dashed-off-points-on-the-nsa-scandal/ (arguing that people will not be moved enough by recent revelations about NSA surveillance to stop voluntarily turning over their information to service providers like Verizon, and as a result that people do not care a great deal about privacy); Eyder Peralta, *In Discussion About Internet Privacy, It Comes Down To Expectation*

There is one further point to address here. Earlier I suggested the possibility that the United States, in essence, has violated the human right to privacy countless times. The analysis below will explore in more detail whether that might be true. But the mere claim that trillions of violations may have occurred[347] already raises a question as to how we understand the notion of a discrete violation of the right to privacy. While this is not the place to elaborate on a philosophical account of the right to privacy, it may be worth addressing how the numbers climb so rapidly, for not all rights conduce to violation in such large batches.[348]

In advancing the possibility of a large number of violations, I consider any single act that could be deemed a violation of Article 17 to be a candidate for the purposes of tallying a hypothetical count. Suppose one sends an email from within the United States to a friend who also happens to be in the United States. Assume that the NSA improperly intercepts the message, saving it in some database. That act could involve at least two violations of the right to privacy: one violation against the sender and one against the recipient. If, as a result of having saved the email without proper authorization, six different analysts read the email, then there might be twelve more violations of the right to privacy: six additional violations against the sender and six more against the recipient.[349] Imagine next that the NSA recognizes that it ought not (legally speaking) to have this email in its database. Perhaps at that point, based on the comments of the Human Rights Committee, failure to delete it generates another pair of violations of the right to privacy (once again, one against the sender and one against the recipient).[350]

Versus Reality, NPR (Feb. 25, 2013, 7:30 PM), http://www.npr.org/blogs/thetwo-way/2013/02/25/172909918/in-discussion-about-internet-privacy-it-comes-down-to-expectation-versus-reality (describing a dissonance between people's expectations of privacy regarding online activity and communications on one hand and the applicable legal standards on the other).

347. *See supra* text accompanying note 18.

348. Again, I thank Faiza Patel for noting the significance of this issue.

349. Matters might get complicated if the same analyst repeatedly accesses the email, or simply maintains constant access to it over some extended period. Perhaps we would call each access a violation, while extended review of the email would involve only a single, particularly egregious violation. I modestly favor the latter position, but there is no need to settle these penumbral issues here.

350. The next natural question would be whether indefinite retention of the email would in itself generate further violations of the right to privacy, or would instead count toward the seriousness of the initial violations. As before, I incline toward

As this example illustrates, a striking feature of the structure of the right to privacy is that a single piece of information or correspondence, if handled improperly, can generate a large number of rights violations. That seems entirely appropriate because if a piece of information is protected as private against many different people, each of those people could engage in discrete violations of the right to privacy by accessing that information improperly. Each piece of protected information constitutes a node that may, in theory, serve as the basis for a substantial number of violations of the right to privacy—sometimes for more than one person at a time, as in the case of protected communications. Given how many pieces of potentially protected information exist about each individual, we might visualize the right to privacy as extending to a substantial web of data points around each person, protecting each point in the web from certain forms of interference or inspection. Indeed, the metaphysical feature of the right that generates this result is not unique to privacy. For example, one person's ownership of a plot of land can ground a large number of discrete trespasses if many different people walk across it (even as a group) without requisite cause or permission.[351] Each plot of land constitutes a node in the web of the owner's property interests, all of which can ground trespasses against the owner. Moreover, in both the privacy case and the trespass case, the discrete trespasses can vary in the extent to which they harm the owner, but that alone does not change the way one counts up the illegal acts.

Violations of other rights manifest differently. Rights not to be tortured[352] or not to be detained arbitrarily[353] attach directly to each protected person and are only violated when a protected person is mistreated. There is only one locus for violations of the right: the person himself. Even in a state that widely tortures or detains people arbitrarily, the number of violations of the rights to be free from such treatment will simply never threaten to approach the number of potential privacy violations that could occur in a state that widely conducts illegal surveillance of its people. That is just a feature of what the right protects against, and thus, the ways in which it can be violated.

---

taking the latter view, but I do not have a definitive intuition on the question.

351. *See* RESTATEMENT (SECOND) OF TORTS § 158 (1965) (offering a definition of trespass compatible with this example, focusing on the actions of each individual).

352. ICCPR, *supra* note 13, art. 7.

353. *Id.* art. 9(1).

The number of violations and the seriousness of each violation are largely independent, but privacy introduces an interesting wrinkle here. If the NSA improperly collects enough data points about a person, the seriousness of the total harm to that person could transcend the seriousness of the harm caused by the collection of each individual piece of information. That is, the whole harm could be greater than the sum of its parts. A distinct fact in isolation may not reveal a great deal that is private about a person, but a collection of information detailed enough to expose further information by implication or by the interaction of its individual data points could reveal exponentially more.

In cases where many violations result from the improper storage and review of a single email, perhaps the large total number of violations appears misleading to the extent that one is naturally primed to infer greater harm from it. But in cases where the large number of violations involves the assembly and deployment of a wide array of data to create detailed pictures of people's activities and preferences, the large number of violations may actually understate the harm. Some of these features of the right to privacy may be helpful in considering the ways in which portions of the NSA program are potentially in conflict with the ICCPR.

V. THE LEGALITY OF THE NSA PROGRAM UNDER ARTICLE 17

A. APPLYING "UNLAWFUL INTERFERENCE"[354]

First, Article 17's prohibition on "unlawful interference" is typically taken to mean that justifiable interference must generally comply with the state's legal system (including "laws, ordinances[,] and judicial directives").[355] At the very least, if the state is interfering with the right to privacy in contravention of its own domestic law, then it is presumptively violating Article 17.[356] As indicated above, one important function of the

354. Though the term "arbitrary" precedes the term "unlawful" in Article 17(1), making it more natural in one sense to analyze arbitrariness first, the fact (as documented above) that the term "arbitrary" reaches further than the term "unlawful" makes it analytically simpler to begin with the latter.

355. NOWAK, *supra* note 21, at 382.

356. A similar result would likely obtain in the ECtHR. *See* HARRIS, O'BOYLE, & WARBRICK, *supra* note 275, at 343-44 (discussing the ECtHR position on policies that

lawfulness requirement is to make sure that interference is "predictable in the sense of the rule of law."[357] Additionally, the Human Rights Committee observes that "[t]he term 'unlawful' means that no interference can take place except in cases actually envisaged by the law. And interference authorized by States can only take place on the basis of law that itself must comply with the provisions, aims and objectives of the Covenant."[358]

Second, a state cannot "avoid its obligation[s] under Art[icle] 17 simply by failing to enact the relevant prohibitive norms or by providing its organs with unreasonably broad discretion for interfering with privacy, since it would thus violate its positive duty of protection set forth in Art[icle] 17(2)."[359]

Although the precise language differs, consider again the jurisprudence of the ECtHR, as Article 8(2) of the European Convention includes the requirement that any interference with the rights laid out in 8(1) be "in accordance with the law and . . . necessary in a democratic society [for the protection of a serious societal interest enumerated in the European Convention]."[360] For the ECtHR, there must be an operative domestic statute governing the surveillance in question; failure of a state to enact a statute governing its surveillance activities can yield the result that those activities are "not in accordance with the law."[361]

Third, Nowak also claims "unlawful" might "cover violations

---

appear to violate the domestic law of the defendant state).

357. NOWAK, *supra* note 21, at 383.

358. General Comment 16, *supra* note 289, ¶ 3.

359. *Id.* In some ways, this suggestion is difficult to comprehend fully, for it implies that the term "lawful" contains at least two elements: first, interference should be sanctioned officially by law, but second, even if it is, the law must meet some independent standard. The first of these elements uses "lawful" in a purely formal sense, while the second uses it in a substantive, normative sense.

360. European Convention, *supra* note 271, art. 8(2).

361. *See Protection of Personal Data*, *supra* note 284, at 8 (discussing *Copland v. United Kingdom*) ("The Court considered that the collection and storage of personal information relating to Ms Copland through her use of the telephone, e-mail and Internet had interfered with her right to respect for her private life and correspondence, and that that interference was not 'in accordance with the law,' there having been no domestic law at the relevant time to regulate monitoring."); *see also id.* at 5 (discussing *Taylor-Sabori v. United Kingdom*) ("Violation of Article 8: there had been no statutory system to regulate the interception of pager messages transmitted via a private telecommunication system.").

of international law binding on the State party concerned."[362] Where there is a statute in place that guides the state in interfering with the right to privacy, that statute can only be valid if it provides "'the minimum degree of protection to which citizens are entitled under the rule of law in a democratic society.'"[363] Luxembourg defeated a challenge to a wiretapping law by stipulating that the European Convention applied to its domestic law, suggesting that the law would have to conform to the Convention even in domestic adjudication; thus, even though potential targets of surveillance were not notified before their phones were tapped, the law required people to have access to general information about when phones *might be* tapped.[364]

In a case called "*Malone*,"[365] the ECtHR came down against the United Kingdom's use of broad administrative authority to design secret surveillance protocols.[366] The court disapproved of the government's ability to change the parameters of its surveillance activities at any time it saw fit.[367] The United Kingdom satisfied the European Commission of Human Rights by adopting a law that provided a statutory basis for its surveillance, even though the corresponding grievance mechanism that it established carved out no role for the courts and made it difficult for complainants to meet the requisite burden of proof.[368]

The NSA program has had a long, complicated relationship with domestic law in the United States, and indeed, the scholarly literature on the program almost exclusively concerns the relationship of the program, in whole or in part, to various pieces of domestic law.[369] Evolving domestic law, incomplete public

---

362. *Protection of Personal Data*, *supra* note 284, at 8.

363. *See* HARRIS, O'BOYLE, & WARBRICK, *supra* note 275, at 340 (internal citations omitted) (reading this as a concern in part about arbitrary use of the power).

364. *Id.* at 340; Mersch v. Luxembourg, App. No. 10439/83, 43 DR 34 (1985).

365. Malone v. United Kingdom, App. No. 8691/79, 7 Eur. H.R. Rep. 14 (1984), *available at* http://www.worldlii.org/eu/cases/ECHR/1984/10.html.

366. HARRIS, O'BOYLE, & WARBRICK, *supra* note 275, at 338-39.

367. *Id.*

368. *Id.* at 339.

369. *See, e.g.*, GREENWALD, *supra* note 60 (arguing that the NSA program is one of several policies enacted by the Bush Administration pursuant to a troublingly broad reading of the United States Constitution); SCHOENFELD, *supra* note 32 (arguing that leaks of national security information are becoming increasingly dangerous and ought to be prosecuted under applicable domestic statutes); Patricia L. Bellia, *The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance Law*, 50 VILL. L. REV. 425 (2005) (discussing the political and constitutional implications of

disclosures, and changes to the program itself all complicate efforts to conduct a clean analysis of the legality of the NSA's efforts under federal statutes. For the present purpose of making an initial foray into underappreciated territory, this Subsection will highlight several major reasons for thinking that the NSA program might have failed (and potentially continues to fail) to

---

changes to the FISA framework making it easier to conduct surveillance on "lone wolf" terror suspects); David Cole & Martin S. Lederman, *The National Security Agency's Domestic Spying Program: Framing the Debate*, 81 IND. L.J. 1355 (2006) (arguing that if federal law is inadequate for the purpose of authorizing the requisite surveillance, the President ought to change the law rather than secretly violating it); Jeremy D. Mayer, *9-11 and the Secret FISA Court: From Watchdog to Lapdog*, 34 CASE W. RES. J. INT'L L. 249 (2002) (arguing that the judiciary has imposed insufficient constraints on surveillance by the U.S. government); Matthew Robinson, *Freedom in an Era of Terror: A Critical Analysis of the USA PATRIOT Act*, 4 JUST. POL'Y J., Spring 2007, *available at* http://www.cjcj.org/uploads/cjcj/documents/freedom_in.pdf (assessing the USA Patriot Act and the implications of the public response for future legislation); Nathan Alexander Sales, *Secrecy and National Security Investigations*, 58 ALA. L. REV. 811 (2007) (recommending adjustments to the domestic legal framework for the use of secrecy in national security investigations); Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287 (2008) (arguing that changes are needed in regulating telecommunications surveillance to balance civil liberties and security concerns better); Richard Henry Seamon, *Domestic Surveillance for International Terrorists: Presidential Power and Fourth Amendment Limits*, 35 HASTINGS CONST. L.Q. 449 (2007) (arguing that under certain conditions the President has constitutional authority to conduct surveillance of the sort done by the NSA, even if doing so violates a duly enacted statute); Tara M. Sugiyama & Marisa Perry, *The NSA Domestic Surveillance Program: An Analysis of Congressional Oversight during an Era of One-Party Rule*, 40 U. MICH. J.L. REFORM 149 (2006) (assessing congressional oversight over the NSA program and finding it generally to be lacking); Bennie J. Thompson, *The National Counterterrorism Center: Foreign and Domestic Intelligence Infusion and the Potential Threat to Privacy*, 6 U. PITT. J. TECH. L. & POL'Y 6 (2006) (arguing for stronger safeguards on the National Counterterrorism Center); Nathan C. Henderson, Note, *The Patriot Act's Impact on the Governments' Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications*, 52 DUKE L.J. 179 (2002) (arguing that the changes made to the domestic legal framework by the USA PATRIOT Act collectively pose a threat to privacy); Jeremy Neff, Note, *Does (FISA + NSA) * AUMF - HAMDI = Illegal Domestic Spying?*, 75 U. CIN. L. REV. 887 (2006) (assessing the argument advanced by the Bush Administration that the NSA program is authorized by the Authorization for Use of Military Force in Afghanistan); Kathleen Clark, The Architecture of Accountability: A Case Study of the Warrantless Surveillance Program (Mar. 11, 2009) (unpublished), *available at* http://works.bepress.com/kathleen_clark/2 (arguing that most of the accountability mechanisms capable of checking the executive branch when it violates the law in fact failed in the case of the NSA program); David S. Kris, Modernizing the Foreign Intelligence Surveillance Act, Brookings Institution, *available at* http://www.brookings.edu/~/media/research/files/papers/2007/11/15%20nationalsecurity%20kris/1115_nationalsecurity_kris (exploring the relationship between modifications to the FISA framework, such as the PAA and the FAA, and technical aspects of various communications).

meet the lawfulness requirement of Article 17. This Article will cover six areas: collection of data beyond the scope intended by the United States government; the extra-legal origins of the NSA program, which bypassed the governing domestic statute (FISA); the numerous doubts as to the legality of the program among government officials; the provision of immunity to complicit private parties; the sheer size and scope of the program; and the outsourcing of surveillance about Americans to friendly foreign governments.

1. ACCIDENTAL OVER-COLLECTION OF DATA

As summarized earlier, there have been a number of instances in which the government has admitted to over-collecting data for the NSA program in violation of the law. Key government admissions of this nature occurred in: late 2005 (just days after the first *New York Times* report on the program), when the government acknowledged having picked up purely domestic phone calls because of a technical glitch and thus without a warrant;[370] April of 2009, when the government acknowledged (perhaps accidentally) stepping outside of the operative legal framework in the collection of Americans' emails;[371] June of 2009, when the *New York Times* reported that the government overstepped its FISC authorization in eight to ten cases (yielding improper collection of potentially millions of communications);[372] August of 2013, when a declassified FISC opinion revealed that the NSA had been using an unconstitutional collection procedure for approximately three years following the passage of the FAA;[373] August of 2013, when the *Washington Post* reported on the May 2012 internal NSA audit revealing nearly 2,800 improper collection or access incidents over the course of the previous twelve months in NSA offices near Washington D.C.;[374] and potentially August of 2013, when the *Wall Street Journal* reported that NSA officers have periodically and improperly used the NSA's capacities to spy on their love interests (depending on whether the officials behind those incidents relied on the post-

370. Risen & Lichtblau, *Spying Program*, *supra* note 109.

371. Lichtblau & Risen, *supra* note 157.

372. Risen & Lichtblau, *E-Mail Surveillance*, *supra* note 162.

373. Nakashima, *supra* note 230.

374. Gellman, *supra* note 223 (reporting the number, and noting that most were unintended).

9/11 program's technical machinery).[375]

These instances appear problematic for the United States' obligations under the ICCPR. Even if these violations of domestic law occurred by accident—and according to news reports, only some of them did—they nevertheless occurred in contravention of the operative legal framework and potentially to the detriment of millions of Americans. Moreover, the fact that the NSA violated domestic law so many times suggests a systemic problem, perhaps a lax approach by the agency toward its international human rights obligations as an arm of the United States government.[376] Indeed, as noted previously, the rate of inadvertent over-collection incidents appears to have increased over the period of the internal May 2012 audit.

Additionally, the Human Rights Committee clearly states what should happen when the government accidentally collects information on individuals improperly: "If [one's personal data, stored in automatic data] files contain incorrect personal data or *have been collected or processed contrary to the provisions of the law*, every individual should have the right to request rectification or elimination."[377] Suffice it to say that the United States has never offered publicly to disclose such information to those wronged by over-collection, nor made clear that it will adjust its databases accordingly by deleting the information that was gathered improperly.[378] Indeed, in the wake of the Supreme Court decision in *Clapper*, Americans have no legal recourse to challenge domestic surveillance under the now-operative FAA if they cannot prove that they were harmed; thus, even justified suspicion that one has had his communications or information improperly collected is insufficient to provide standing to bring a

375. Gorman, *NSA Love Interests*, *supra* note 236. Note that Sen. Feinstein claimed to have seen no evidence suggesting that LOVEINT "involved the use of NSA's domestic surveillance infrastructure." *Id.*

376. Recall that lawfulness under domestic law is a requisite for interference with privacy under the ICCPR. *See* ICCPR, *supra* note 13, art. 17.

377. General Comment 16, *supra* note 289, ¶ 10 (emphasis added); *see also* U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, Fourth Periodic Report (France)*, ¶ 22, U.N. Doc. CCPR/C/FRA/CO/4 (July 31, 2008) (reiterating the same point).

378. It is worth noting, however, that there is at least one reported instance of the NSA "purging" improperly collected information, which took place in April of 2012, a few months after the agency had satisfied the FISC that it had replaced its unconstitutional search provision. Nakashima, *supra* note 230.

legal claim.[379]

2. EXTRA-LEGAL INITIATION OF THE PROGRAM

A second way in which the NSA program may run afoul of the lawfulness requirement is through the fact that the initial implementation of the program in 2001 completely bypassed the widely recognized legal framework for conducting domestic surveillance—that is, it was conducted outside of FISA (even as modified by the USA PATRIOT Act), with the government leaving the FISC out of the loop. Americans who communicated with parties abroad were subject to warrantless surveillance, notwithstanding FISA's prohibition of such conduct and the attendant clause that identified FISA as the sole means by which domestic surveillance for foreign intelligence purposes may be conducted.[380] The government has maintained that it nevertheless has the authority to initiate the program, under broad theories of executive power and, indirectly, under the Authorization of Use of Military Force (AUMF) passed by Congress in 2001 to permit the government to use force against those responsible for the 9/11 attacks.[381]

Whether or not the executive branch possesses such power has been a matter of substantial debate,[382] and it is not easy to

---

379. Clapper v. Amnesty Int'l USA, 568 U.S. ___, 133 S. Ct. 1138 (2013).

380. *See* 18 U.S.C. § 2511(2)(f) (2008).

381. *See, e.g.*, GREENWALD, *supra* note 60, at 38 (arguing that a broad reading of presidential power underlies the NSA program, among other policies established by the Bush Administration); *see* Sugiyama & Perry, *supra* note 111, at 157 (citing congressional testimony by former Attorney General Alberto Gonzalez as evidence that the Bush Administration claimed power to undertake the NSA program through the AUMF).

382. *See, e.g.*, GREENWALD, *supra* note 60, at 36-37 (arguing that the statutory language clearly and conclusively bars some of the activities of the NSA during the early era of the program); Seamon, *supra* note 369, at 504 (arguing that under certain conditions the President has constitutional authority to conduct surveillance of the sort done by the NSA, even if doing so violates a duly enacted statute); Sugiyama & Perry, *supra* note 111, at 157 (noting the congressional testimony of former Attorney General Alberto Gonzalez to the effect that authority for the NSA program derives from the AUMF); Jay Bybee, Memorandum to Alberto R. Gonzales, Counsel to the President (The "Torture Memo") § 5, at 31-38, *available at* http://www.tomjoad.org/bybeememo.htm (last visited Feb. 3, 2014) (arguing, among other things, that parts of the United States Code that appear to restrict the authority of the government to engage in aggressive interrogation of enemy combatants may constitute an unconstitutional infringement on the president's powers as commander-in-chief.). For background on the question of the president's constitutional authority, see Lawrence Lessig & Cass R. Sunstein, *The President and*

reach an uncontroversial conclusion. But it may not matter a great deal for present purposes. To the extent that the lawfulness requirement of Article 17 factors in whether interference is "predictable in the sense of rule of law,"[383] the NSA's secret bypassing of FISA between 2001 and 2005 was clearly problematic.[384] This is all the more true because President Bush publicly endorsed the USA PATRIOT Act in 2001 as providing sufficient updates to the legal framework for surveillance so as to make it possible to fight the War on Terror.[385] In fact, Bush Administration officials claimed that warrants remained necessary for conducting domestic surveillance.[386] While such statements may have deceived would-be terrorists into thinking that their data and communications were only being collected to the extent permitted by the FISA framework (as modified by the USA PATRIOT Act), they also deceived the innocent. The ensuing collection of Americans' foreign communications was not predictable because the law—as understood by nearly everyone outside the executive branch—explicitly prohibited it.[387]

As we have seen, once the program was disclosed, the government made various efforts to update the domestic legal framework to enable it to continue the program with fewer doubts about the legality of its activities—culminating, for now, in the passage of the FAA in 2008 and its recent renewal. At various points, as the scope of the law expanded, greater portions of the program presumably began to fall under its coverage. Yet questions still remain as to whether the law provides predictability in any meaningful sense. David Kris, a former Assistant Attorney General with the National Security Division of the Justice Department, has long claimed that the government interprets the FAA to permit the collection of purely domestic communications if that collection is done in service of gathering information on a legitimate target.[388] Reporting from August

---

the Administration, 94 COLUM. L. REV. 1 (1994).

383. NOWAK, *supra* note 21, at 383.

384. Warrantless surveillance continued after 2005, potentially up to 2008 and even to the time of this writing, but as of the end of 2005, the public was on notice that the government had adopted the practice.

385. GREENWALD, *supra* note 60, at 14.

386. Risen & Lichtblau, *supra* note 4.

387. Additionally, judges who have reached the question have enforced FISA's exclusivity clause as legally binding, as we will discuss below.

388. David Kravets, *House Approves Sweeping, Warrantless Electronic Spy Powers*,

2013 seems to confirm that reading, though the FISC has ruled at least some such collection unconstitutional.[389] Even with some limitations imposed by an irritated FISC, that interpretation of the FAA continues to deny Americans genuine predictability, especially in light of public statements by the head of the NSA denying the agency's technical ability to capture purely domestic communications.[390] In short, there is no meaningful sense in which the information being gathered on Americans is predictable under domestic law. Moreover, because *Clapper* has rendered it particularly difficult to mount a challenge to the constitutionality of the FAA, questions remain as to whether the applicable domestic law is in fact valid under the United States Constitution.

3. SKEPTICISM OF THE PROGRAM'S LEGALITY FROM GOVERNMENT OFFICIALS

Third, and as a related matter, the opinions of government officials on the legality of the program are far from uniform. Recall in particular that judicial opinions are relevant for determining whether a program is "lawful" under Article 17, pertaining as they do directly to the standing of the law.[391] Three federal judges have, at various points, ruled against the program. In August of 2006, Judge Anna Taylor Diggs of the Eastern District of Michigan ruled (in *ACLU v. NSA*) that the NSA program violated both FISA and the United States Constitution.[392] Her ruling concerned the program in its form as originally disclosed in 2005—when it involved entirely warrantless collection of emails and phone calls between a party within the United States and a party abroad.[393]

WIRED, Sept. 12, 2012, http://www.wired.com/threatlevel/2012/09/house-approves-spy-bill/.

389. *See supra* text accompanying note 233.

390. *See, e.g.*, Greenberg, *supra* note 176 (detailing General Alexander's testimony before Congress about the NSA's inability to conduct certain domestic surveillance). In that testimony, Alexander explicitly claimed that the "NSA does not have the ability" or "capacity" to identify the American parties to a domestic email exchange, lacking the requisite "technical insights into the United States." *Id.*

391. NOWAK, *supra* note 21, at 382 (noting the relevance of "judicial directives").

392. Am. Civil Liberties Union v. Nat'l Sec. Agency, 438 F. Supp. 2d 754, 782 (E.D. Mich. 2006), *vacated*, 493 F.3d 644 (6th Cir. 2007); *see* Dan Eggen & Dafna Linzer, Judge Rules Against Wiretaps, WASH. POST, Aug. 18, 2006, http://www.washingtonpost.com/wpdyn/content/article/2006/08/17/AR2006081700650.html.

393. *See* Eggen & Linzer, *supra* note 392.

That decision was vacated a year later by the United States Court of Appeals for the Sixth Circuit, which (in a 2–1 decision that foreshadowed *Clapper*) found that the plaintiffs lacked standing to challenge the program because they could not show that they had been harmed by it.[394] In his dissent, Judge Ronald Gilman voted to affirm Judge Diggs's decision, agreeing that the NSA program was illegal.[395] At the time, Glenn Greenwald observed that in finding standing for the plaintiffs, Judge Gilman became both the second non-FISC judge to assess the program and the second to find it illegal.[396]

In 2010, Judge Vaughn Walker of the Northern District of California became the third non-FISC judge who reached the merits of an NSA program-question to find the program illegal.[397] He ruled that the government violated FISA when, without a warrant, it intercepted the international phone calls of an Oregon-based Islamic charity.[398] The case did not raise questions about standing because the charity was able to marshal public information to prove that it had been subjected to warrantless surveillance.[399] The ruling once again counted toward the illegality of the government's efforts to gather communications of Americans without following the FISA warrant procedures.

Beyond the judiciary, a number of government officials have expressed serious concerns about the legality of the NSA program. Perhaps most strikingly, the Bush Administration's decision to reauthorize the program despite opposition from the Office of Legal Counsel nearly prompted mass resignations at the Department of Justice in 2004, according to a high-placed official in the Administration.[400] At the time, the Office of Legal Counsel

394. Am. Civil Liberties Union v. Nat'l Sec. Agency, 493 F.3d 644, 648 (6th Cir. 2007) (Gilman, J., dissenting).

395. *Id.* at 693-720 (agreeing that the program was in violation of FISA).

396. Glenn Greenwald, *The criminal NSA eavesdropping program*, SALON (Apr. 1, 2010, 7:02 AM), http://www.salon.com/2010/04/01/nsa_4/.

397. *Id.*

398. Charlie Savage & James Risen, *Federal Judge Finds N.S.A. Wiretaps Were Illegal*, N.Y. TIMES, Apr. 1, 2010, http://www.nytimes.com/2010/04/01/us/01nsa.html?ref=foreignintelligencesurveillanceactfisa&_r=0.

399. *Id.*

400. *See U.S. Senate Judiciary Committee Holds a Hearing on the U.S. Attorney Firings*, 110th Cong. 10-25, 18 (2007) (statement of James Comey, Former Dep. Att'y Gen. of the United States) [hereinafter Comey Testimony], *available at* http://gulcfac.typepad.com/georgetown_university_law/files/comey.transcript.pdf (describing the incident).

was evaluating the legal basis for the NSA program, which at that point required the periodic approval of the Attorney General.[401] The reason for the review by the Justice Department is not clear, but it could relate to the complaints of FISC Judge Kollar-Kotelly about the government's use of information obtained from the NSA program to secure FISA warrants in other cases (discussed above).[402] Attorney General John Ashcroft and his deputy James Comey had come to the conclusion that they could not certify the NSA program as legal.[403] When the Bush Administration nonetheless decided to reauthorize the program, a large number of people at the Department of Justice—and even the FBI Director—prepared to resign.[404] The Administration ultimately backed off, accepting changes to the program requested by the Department of Justice.[405]

A number of other government officials have also expressed concerns at various points about the legality of the NSA program, including former Assistant Attorney General David Kris,[406] former NSA crypto-mathematician James Binney,[407] and certain FBI personnel (including former FBI director Robert Mueller).[408] Numerous legislators have expressed the view that the program is or may be illegal, including Senators Russ Feingold, Jack Reed, Arlen Specter,[409] Rand Paul,[410] Jeff Merkley, Bob Corker, Mark

---

401. *Id.* Note that Comey refused in his testimony to identify which program he was describing, but subsequent reporting seems to confirm that it was the collection of Americans' email under the NSA program that caused the controversy. Risen & Lichtblau, *E-Mail Surveillance*, *supra* note 162.

402. *See supra* text accompanying note 90.

403. Comey Testimony, *supra* note 400. The series of events surrounding the decision by Ashcroft and Comey was surprisingly dramatic. Hours after they jointly decided not to recertify the program, Ashcroft became very ill and was admitted to the intensive care unit at a local hospital, making Comey the acting Attorney General. *Id.* Comey communicated to the White House that he would not certify the program, so White House Counsel Alberto Gonzalez and President Bush's Chief of Staff Andrew Card attempted to visit Ashcroft in intensive care to get him to overrule Comey. *Id.* Comey learned of their plans and raced to the hospital, arriving minutes before them and setting up a tense confrontation. *Id.*

404. *Id.*

405. *Id.*

406. Kravets, *supra* note 388.

407. Bamford, *NSA Spy Center*, *supra* note 79.

408. Comey Testimony, *supra* note 400; Lichtblau & Risen, *supra* note 157.

409. *Inquiry into leak of NSA spying program launched,* CNN (Dec. 30, 2005, 9:26 PM), http://www.cnn.com/2005/POLITICS/12/30/nsa.leak/.

410. *See* Molly Reilly, *Rand Paul: NSA Surveillance Programs Warrant Supreme Court Challenge,* HUFFINGTON POST (June 9, 2013, 10:32 AM),

Udall,[411] and (arguably) Ron Wyden,[412] as well as Representatives Rush Holt[413] and Justin Amash.[414]

Thus, there is good reason to believe that the NSA program is not, or has not always been, consistent with United States domestic law. Many of the concerns from government officials, including judges, predated the passage of the FAA and related to the use of the program to sidestep the FISA framework (as in the various federal court rulings and the revolt at the Department of Justice). At the very least, then, until the domestic legal framework caught up to the program (whether that occurred with the PAA in 2007 or the FAA in 2008), there is a nontrivial probability that parts of the program were simply illegal under domestic law—and, accordingly, the ICCPR.

4. LEGAL IMMUNITY OF IMPLICATED PRIVATE PARTIES

Fourth, one of the most controversial aspects of the FAA of 2008 was that it retroactively and prospectively immunized private parties involved in the NSA program.[415] Those provisions were especially valuable to major telecoms, many of which began turning over calling records and assisting the government in conducting warrantless surveillance. While the telecoms had acted at the request of the government, they were vulnerable to civil and criminal liability under the original FISA statute.[416]

---

http://www.huffingtonpost.com/2013/06/09/rand-paul-nsa_n_3411587.html (reporting on Senator Paul's interest in challenging the NSA program at the Supreme Court level).

411. *See* Sam Stein & Michael McAuliff, *NSA Collection Of Verizon Phone Records Defended By Top Senators*, HUFFINGTON POST (June 6, 2013, 12:50 PM), http://www.huffingtonpost.com/2013/06/06/verizon-phone-records-nsa_n_3397058.html?utm_hp_ref=politics (quoting Senators Merkley, Corker and Udall all expressing reservations about the permissibility of the program).

412. *See, e.g.*, Jathan Sadowski, *Ron Wyden's Warning: America May Be on Track to Become Surveillance State*, SLATE (July 23, 2013, 5:05 PM) http://www.slate.com/blogs/future_tense/2013/07/23/ron_wyden_dangers_of_nsa_surveillance_and_the_patriot_act.html (quoting Wyden's deep concerns about the NSA program's implications for our "constitutional history").

413. Risen & Lichtblau, *E-Mail Surveillance*, *supra* note 162.

414. *See* Weisman, *supra* note 239 (referring to Amash's opposition to the program as reflecting his concerns about of its conformity to the requirements of the Fourth Amendment to the United States Constitution); *FISA Amendments Act of 2008*, WALL. ST. J. (June 19, 2008, 6:24 PM), http://online.wsj.com/news/articles/SB121391360949290049.

415. Hess, *supra* note 10.

416. *Id.*

While it is hard to imagine that the government would prosecute the companies under a law it too had circumvented, particularly in light of the companies' cooperation, forty-six civil suits were pending against the telecoms when the FAA took effect,[417] collectively seeking hundreds of billions in damages.[418] The law's immunity provisions abruptly preempted all of these suits.[419]

The fact that the telecoms were vulnerable to civil liability in the first place is highly suggestive, though not determinative, of legal transgressions on their part. After all, if it were reasonably clear that they had not broken any laws, retroactive immunity would have been unnecessary and there probably would not have been nearly four-dozen pending lawsuits against them. This point is relevant in two respects. First, and most obviously, it contributes to the sense that the original instantiation of the program was illegal under domestic law.

Second, recall Nowak's discussion of the positive obligations on states under Article 17.[420] The Human Rights Committee has also discerned those positive obligations: "States parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal persons."[421] Although the passage of FISA in 1978 predated the relevant commentary of the Committee, FISA's terms would arguably satisfy the Committee's interpretation. However, retroactively immunizing those private actors who then violated the law runs completely against the grain of the state's positive obligation to ensure protection of the rights that even the domestic law plainly recognized. To the extent the FAA rolls back the liability of private actors for violations of the right to privacy, it constitutes an affirmative step *against* the dictates of Article 17: it encourages private actors to participate in the violation of the right to privacy rather than incentivizing them to respect it.

5. SCOPE AND INDISCRIMINATE NATURE

Fifth, the NSA program has grown so large that it is unclear

417. Hess, *supra* note 10.

418. Recent Legislation, 122 HARV. L. REV. 1271, 1271 (2009).

419. Hess, *supra* note 10.

420. *See supra* text accompanying note 268.

421. General Comment 16, *supra* note 289, ¶ 9.

if it meets the substantive requirements of the lawfulness clause of Article 17, even to the extent that the program has, since 2008, been governed by a domestic statute. As the Human Rights Committee has explained, "[i]nterference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant."[422] It is not at all obvious that the FAA conforms to the provisions, aims, or objectives of the ICCPR. As noted above, it allows for officials from the executive branch—not judges—to issue broad, yearlong warrants that target individuals and groups abroad. Moreover, as reporting in August of 2013 has revealed, the government interprets the FAA to permit the collection of communications between individuals who are not suspected of any wrongdoing but whose correspondence might be relevant to an investigation of targeted individuals. Additionally, Verizon has been turning over all of its calling records to the government, which is also gathering hundreds of millions of transactional data points about a wide range of Americans' activities.[423] Even presuming these practices are permissible under domestic law, the indiscriminate nature of such data collection raises a similar concern as the broad FAA warrant provision. (This is, in some ways, the second complaint one might raise against the immunity provision, but here it is applied to the targeting provisions of the FAA and the business records provision of the USA PATRIOT Act.)[424]

These are not merely abstract worries. The Human Rights Committee has articulated standards for legislation with respect to the protection of correspondence:

> Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis. Compliance with article 17 requires that the integrity and confidentiality of

422. General Comment 16, *supra* note 289, ¶ 3.

423. Greenwald, *NSA collecting phone records*, *supra* note 2.

424. See, e.g., U.N. Human Rights Comm., Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, Second and Third Periodic Reports (USA), ¶ 21, U.N. Doc. CCPR/C/USA/CO/3/Rev.1 (Dec. 18, 2006) (expressing concern about the USA PATRIOT Act even before recent disclosures revealed the government's broad interpretation of Section 215, the "business records" provision of the Act).

> correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.[425]

Under the FAA, it seems as if most of these requirements are subject to frequent violation. Note in particular the demand that authorized interference should be approved on a case-by-case basis. The broad intercept orders permitted by the FAA are not nearly that targeted.[426] Note also the requirement that legislation ought to spell out the precise conditions that would permit interference. Under the FAA, the Attorney General and the Director of National Intelligence secretly submit their targeting provisions to the FISC, so that information is rarely available to the public.[427]

6. OUTSOURCING OF IMPERMISSIBLE SURVEILLANCE

Sixth, and finally, recall the discussion of the United States position on the territorial scope of the ICCPR,[428] and in particular, its view that its duties under the ICCPR extend only to those within both its territory and jurisdiction. We have proceeded on the assumption that the United States' interpretation is the correct one—not out of agreement with that position (which is both at odds with the position of the Human Rights Committee and maximally restrictive vis-à-vis the ICCPR), but because doing so shows that even under less controversial assumptions, there appear to be serious problems for the legal position of the United States. After all, a primary point of focus in the controversy about United States government surveillance has been its ability to gather information directly about people within its territory and subject to its jurisdiction.[429]

---

425. U.N. Human Rights Comm., *supra* note 424, ¶ 8.

426. *See* ACLU Letter, *supra* note 3 (criticizing the law for allowing extremely broad, non-particularized warrants).

427. 50 U.S.C.S. § 1881a (2008) (explaining submission to the FISC).

428. *See supra* Section III(A).

429. To the extent that the controversy has concerned either the United States Constitution or FISA, this is effectively true by definition. Indeed, several of the sources cited above—see, for example, CHURCH COMMITTEE REPORT, *supra* note 22; Cauley, *supra* note 81; ELEC. FRONTIER FOUND., *supra* note 114; Nakashima, *supra*

But there have also been allegations that the United States bypasses some concerns about conducting domestic surveillance by collaborating with *other countries* that gather information on Americans.

James Bamford has detailed some of these allegations in his reporting for *Wired Magazine*, in which he notes that the United States has very close relationships with Canada, the United Kingdom, Australia, and New Zealand.[430] He claims that these five countries frequently collaborate on matters of surveillance, referring to themselves (in rather Orwellian fashion) as the "Five Eyes."[431] According to Adrienne Kinne, the former voice interceptor referred to in other reporting by Bamford, this group of countries had an agreement prior to 9/11 not to spy on each other's citizens; however, that has changed, and these governments now frequently act on requests to perform surveillance for each other.[432]

If Bamford's reporting is accurate, then the United States could be taking advantage of the fact that although its domestic legislation regulates its own conduct on its own soil, that legislation does not reach the behavior of other countries. But the ICCPR does not make any such distinction. If the United States cannot actually protect Americans' information and communications from interception by foreign governments (and if those countries have no obligations under the ICCPR to abstain from collecting that information, as the United States' position would seem to imply), it would still seem completely in tension with the object and purpose of the treaty for the United States simply to outsource impermissible domestic surveillance to foreign parties that are, in its view, free from the same restrictions.

B. APPLYING "ARBITRARY INTERFERENCE" TO THE NSA PROGRAM

The disjunctive phrasing of Article 17(1) clearly implies that

---

note 230; *An Impeachable Offense?*, *supra* note 45—all refer in their titles specifically to the interests of Americans. The DOJ controversy that nearly resulted in mass resignations appears to have concerned the privacy rights of Americans as well. *See supra* note 401.

430. Bamford, *Whistleblowers*, *supra* note 176.

431. *Id.*

432. *Id.*

lawfulness and non-arbitrariness are both necessary conditions for permissible state interference with the right to privacy (barring certain general exceptions)—and that the two terms are not coextensive.[433] Indeed, this is the position taken by Volio[434] and Nowak.[435] Volio claims that while "arbitrary" can imply "unlawful," it also means "capricious, despotic, imperious, tyrannical, or uncontrolled. . . . [A]s well as 'incompatible with the principles of justice' and human dignity."[436] More precisely, "[a]ction may be arbitrary even when it is not a violation of positive law if the legislation is itself unreasonable or capricious."[437] Nowak observes that during the debates about how to interpret the two words, "it was stressed above all that 'arbitrary' clearly went beyond 'unlawful' and contained an element of 'capriciousness.'"[438] The ICCPR draws the term from Article 12 of the UDHR, and according to Nowak, it contains "elements of injustice, unpredictability and unreasonableness."[439]

Perhaps most significantly, the Human Rights Committee itself views "unlawful" and "arbitrary" as providing different coverage:

> In the Committee's view the expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.[440]

The Committee has further developed its Article 17 definition of "arbitrary" through case law. In *Canepa v. Canada*, it held that "arbitrariness . . . is not confined to procedural arbitrariness, but extends to the reasonableness of the interference with the person's rights under Article 17 and its

---

433. *See* ICCPR, *supra* note 13, art. 17(1) ("No one shall be subject to arbitrary or unlawful interference . . . .").

434. Volio, *supra* note 261, at 191.

435. NOWAK, *supra* note 21, at 382.

436. Volio, *supra* note 261, at 191.

437. *Id.*

438. *Id.* at 382.

439. *Id.* at 382-83.

440. General Comment 16, *supra* note 289, ¶ 4.

compatibility with the purposes, aims and objectives of the Covenant."[441]

Aside from the controversial "extra-legal" beginnings of the NSA program, another major point of concern from critics is precisely that it is arbitrary. There are several ways in which the program might trigger concern under the "arbitrariness" prong of Article 17: through the accidental over-collection of information; the sheer breadth of the program; and the initial warrantless phase of the program.

1. ACCIDENTAL OVER-COLLECTION OF DATA

Accidental over-collection of data bears on lawfulness, as discussed above, but it is also arbitrary by definition (even in the subset of cases where it is also legal under domestic law) because it is not executed for cause. Such collection would be especially problematic in those cases lacking a legitimate auxiliary justification for collecting the data, but it is troubling in any form. Moreover, the consistency with which errors at the NSA result in over-collection of data—thousands of times per year in D.C.-area offices alone—reveals a systemic problem with significant implications for the covenant's non-arbitrariness requirement.

Additionally, recall further the allegations of a former NSA analyst that the agency had gained warrantless access to Americans' emails through a large database called "Pinwale," beginning as early as 2005.[442] The analyst claimed that the agency would run searches in the database and accept an incidental yield of Americans' communications as high as thirty percent.[443] These claims suggest a protocol that routinely permitted the substantial, unintended over-collection of data in a manner that does not itself register as a problem within the NSA. Such collection would seem to be arbitrary in the sense of lacking cause, and it is unlikely to be reported as an "incident" on an internal audit because it falls within the agency's defined parameters for acceptable rates of error.

---

441. Canepa v. Canada, Comm. No. 558/1993, ¶ 11.4, U.N. Doc. CCPR/C/59/D/558/1993 (June 20, 1997), *available at* http://www1.umn.edu/humanrts/undocs/558-1993.html, *quoted in* NOWAK, *supra* note 21, at 384.

442. Risen & Lichtblau, *E-Mail Surveillance*, *supra* note 162.

443. *Id.*

2. SCOPE AND INDISCRIMINATE NATURE

Just as the NSA program's overwhelming size raises concerns that it is unlawful, as discussed above, the implications of the program's size for the applicable standards of suspicion introduces arbitrariness concerns as well. The NSA has a *reason* for wanting to collect as much information as possible, which differentiates massive, deliberate collection from systematic if unintended over-collection; however, given the sensitivity of the information sought, merely finding utility in collecting the information is unlikely to save the program from violating the non-arbitrariness restriction. The allegations of David Kris and James Binney are particularly relevant here, but even if one takes a skeptical position on their claims, the *Washington Post*'s report that close to 2 billion calls and emails are intercepted every day raises questions about how the collection could fail to be capricious.[444] More recently, according to the *Washington Post*, the NSA has gathered 250 million Internet communications through § 702 of the FAA alone.[445] The NSA also (very quickly) copies and searches communications between "untargeted" individuals to see if they refer to targeted individuals or matters. Both of these facts are strongly suggestive of arbitrariness in a substantive sense: they reveal deeply intrusive practices that affect people who are not at all suspected of wrongdoing.

The same point stands with respect to the collection of transactional data.[446] Recall Binney's claims that AT&T turned over all of its calling records (in addition to providing wiretap access to ongoing calls)[447] and the reporting in the *Wall Street Journal* concerning collection of financial data and other private

444. Binney's estimate that 15 to 20 trillion communications have been collected since 9/11 would support the same conclusion. Of course, on the United States' conservative reading of the territorial scope of the ICCPR, some subset of these communications might be fair game under the ICCPR. But, to the extent that reporting has repeatedly confirmed huge volumes of domestic American communications being caught up in the dragnet, the ultimate conclusion remains the same.

445. Craig Timberg & Barton Gellman, *NSA paying U.S. companies for access to communications networks,* WASH. POST, Aug. 29, 2013, http://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story_1.html.

446. If anything, the apparently lower domestic legal standards for securing transactional data would seem to provide even more cause for concern on this score.

447. *See* Bamford, *NSA Spy Center*, *supra* note 79.

"transactional" details about individuals.[448] Recall also that Verizon has been turning over all of its transactional calling data, regardless of whether the data pertain to people who are under suspicion. The Human Rights Committee has taken a position on the collection of such data, stipulating that ". . . the competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant."[449] Untargeted collection of the sort documented above is so broad that it would seem impossible to escape the conclusion that it is arbitrary in the sense defined by Nowak, Volio, and the Human Rights Committee.

3. INITIAL WARRANTLESS STAGES OF THE PROGRAM

Finally, any interference with the right to privacy that occurs without a warrant is, in some sense, arbitrary, particularly in a system that places a premium on due process guarantees. The term "warrant" implies proper authorization, and warrants play a crucial role in shielding Americans from unreasonable searches in United States constitutional law. As discussed in substantial detail above, the first several years of the NSA program involved the substantial, warrantless collection of personal data. Additionally, for six months in late 2007 and early 2008, under the PAA, executive branch officials (rather than judges) issued the targeting authorizations for the NSA program—both for foreigners and for Americans. As a result, these authorizations may not have amounted to warrants in any meaningful sense.[450] Even now, under the FAA, executive

448. *See* Gorman, *NSA's Domestic Spying*, *supra* note 79.

449. General Comment 16, *supra* note 289, ¶ 7.

450. *See, e.g.*, U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, Fourth Periodic Report (Netherlands)*, ¶ 15, U.N. Doc. CCPR/C/NLD/CO/4 (Aug. 25, 2009) (urging The Netherlands to "amend its legislation to ensure that its counter-terrorism measures do not conflict with article 17 of the Covenant and that effective safeguards, including judicial oversight, are in place to counter abuses"); U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, Sixth Periodic Report (Sweden)*, ¶ 18, U.N. Doc. CCPR/C/SWE/CO/6 (May 7, 2009) ("The State party should take all appropriate measures to ensure that the gathering, storage and use of personal data not be subject to any abuses, not be used for purposes contrary to the Covenant, and be consistent with obligations under article 17 of the Covenant. To that effect, the State party should guarantee that the processing and gathering of information be subject to review and supervision by an independent body with the necessary guarantees of impartiality and effectiveness.").

officials continue to issue warrants for foreign targets, raising the same issues. Moreover, those FAA warrants are broad and yearlong, making them so sweeping that they appear to allow the collection of largely incidental private information relating to people who are suspected of no wrongdoing whatsoever. The link between the authorization and the collection is so tenuous that these collections are "warranted" only in the loosest sense of the word. As a result, the FAA itself may violate the ICCPR. Similarly, Bamford has alleged that there are approximately one million people on agency watch lists.[451] The standard for suspicion must be quite low if so many people clear the bar; if the standard itself is *sufficiently* low, the law that codifies it could well be arbitrary.

VI. DRAWING SOME CONCLUSIONS

Both the Human Rights Committee and Manfred Nowak argue that Article 17 permits interference with the right to privacy only when it is lawful, non-arbitrary, and proportionate to the pursuit of a legitimate aim.[452] The preceding analysis highlights a number of ways in which the NSA program seems both unlawful and arbitrary: fatal flaws under the dominant interpretation of Article 17. Even if the United States were to take the position—in good faith—that the NSA program is essential for national security, the standard analysis would seem to suggest that the program needs substantial revisions to bring it into line with the terms of the ICCPR.

We have already foreclosed the possibility that national security could justify unlawful and arbitrary interference with the right to privacy; that reading is implausible because of its implications, not to mention the fact that it is in tension with the

---

451. Bamford, *NSA Spy Center*, *supra* note 79.

452. *See* Special Rapporteur Report, *supra* note 294, ¶ 28 ("The framework of article 17 of the ICCPR enables necessary, legitimate and proportionate restrictions to the right to privacy by means of permissible limitations."); *International Principles on the Application of Human Rights to Communications Surveillance*, NECESSARY & PROPORTIONATE (July 2013), *available at* https://en.necessaryandproportionate.sorg/text#_edn2 (offering, in the Preamble, a general statement of principles for guiding the right to privacy across international human rights law, and using a similar formulation). This Article has not focused on proportionality—a largely secondary, empirical question that the preceding analysis suggests we need not reach, given the myriad ways in which the program appears to conflict with the direct language of the ICCPR. Nevertheless, the truly massive size of the program would set a high bar for any countervailing considerations necessary to establish proportionality.

major interpretations of the ICCPR and the European Convention. But perhaps there is a more promising indicator for the United States in the deference shown by the ECtHR where states parties assert national security as the justification for their interference with the right to privacy.

Recall that the ECtHR places substantial weight on the existence of "formal legality and procedural guarantees."[453] More specifically, in addition to insisting that the state act in accordance with its own domestic laws (thus ensuring formal legality), clarity about the "scope and manner of exercise" of the state's activities are important considerations in assessing the permissibility of interference with the right to privacy under Article 8 of the European Convention.[454] If those conditions are met, and the purpose of the interference is legitimate (such as protecting national security), then the ECtHR is likely to defer to the state actor.

Even here, however, the United States would struggle. Set aside the fact that, for much of its duration, the NSA program lacked formal legality. Perhaps more significantly, even now the program has weak procedural guarantees, with (among other things) a limited role for the courts, frequent over-collection of information by the government, and only the most modest of roles for particularized suspicion in targeting. Moreover, as the ongoing leaks about the program demonstrate, many of the government's activities remain hidden from public view, necessarily rendering impossible a wide understanding of their nature and scope. Perhaps the United States could modify the NSA program in a way that would allow it to retain its breadth while also complying with the sorts of criteria valued by the ECtHR. Perhaps the government could reveal the program more fully to the public. But until and unless that happens, a favorable verdict by analogy is unlikely.

In sum, it is obviously difficult to reach conclusive opinions about the legality of the NSA program (or its various constituent parts) under the ICCPR in part because some of our analysis is built on credible but disputed reporting on the program itself. At the very least, we need additional, concrete information about how the government executes the program. Further, the

453. HARRIS, O'BOYLE, & WARBRICK, *supra* note 275, at 354.

454. *See supra* text accompanying note 317.

arguments on either side are relatively complicated and can develop in a range of different ways. But at a minimum, even on conservative assumptions about the nature of the program and the scope of the ICCPR, we face the legitimate and frightening prospect that the United States is systematically and massively violating the human right to privacy.

What happens now? Selective leaks in the media help to shed light on parts of the program, but the government is unlikely to turn over any more comprehensive information voluntarily. The limited congressional oversight that occurred shortly after the program became known fell far short of the public accountability created by investigations into spying abuses in the mid-1970s. Despite a string of recent revelations, the current political climate is even less likely to lead to significant oversight than it was in 2005 and 2006, as administrations of both parties have now formally endorsed the FAA, thereby illustrating their commitment to the NSA program.

But suppose we look at the issue from another angle. Why is it that the arguments on both sides are so complicated and uncertain? In part, the reason is that international human rights bodies have not paid enough attention to the risks posed to privacy by government surveillance programs. We have inferred the various points of illicit contact between the NSA program and the ICCPR by carefully reading both news reports about the program and commentaries on the treaty. But the Human Rights Committee's General Comment on the right to privacy is over twenty-five years old, and no more than two-pages long; it lacks important detail, and does not specifically address surveillance practices that are certain to be in wide use around the world today.

This Article essentially presents a case study about the human right to privacy in the United States, as implicated by a single—albeit major—national security initiative. The NSA has multiple surveillance programs, and it is not the only agency within the U.S. government that conducts surveillance here. Most importantly, other countries conduct their own surveillance, making this a global issue. Governments can discern the basic form of their human rights obligations; they cannot be excused for ignoring those obligations simply because it is possible to obscure their activities behind the cloak of national security policy. Nevertheless, it is much easier for them to duck their obligations

when they can claim ambiguity in the law.

If human rights bodies were to take the matter seriously, Articles like this one would not be necessary. Governments will continue to hide information about their surveillance activities, and it may be difficult to change that. But emphasis by human rights bodies on the significance of the right to privacy, and the elaboration of clear standards for compliance with it, would constitute crucial steps in ensuring that states do not trample on this core human right.