2015

Surveillance, Secrecy, and the Search for Meaningful Accountability

Sudha Setty
Western New England University School of Law, ssetty@law.wne.edu

SURVEILLANCE, SECRECY, AND THE SEARCH FOR MEANINGFUL ACCOUNTABILITY

SUDHA SETTY*

One of the most intractable problems in the debate around maintaining the rule of law while combating the threat of terrorism is the question of secrecy and transparency. In peacetime, important tenets to the rule of law include transparency of the law, limits on government power, and consistency of the law as applied to individuals in the polity. Yet the post-9/11 decision-making by the Bush and Obama administrations has been characterized by excessive secrecy that stymies most efforts to hold the government accountable for its abuses. Executive branch policy with regard to detention, interrogation, targeted killing, and surveillance are kept secret, and that secrecy has been largely validated by a compliant judiciary that has dismissed almost all suits challenging human and civil rights abuses resulting from counterterrorism programs. Efforts by Congress to engage in meaningful oversight have met with mixed results; in the area of government surveillance, such efforts have been fruitless without the benefit of leaked information on warrantless surveillance by government insiders. The executive branch has generally refused to make public vital aspects of its surveillance programs in ways that could give oversight efforts more muscle. At the same time, the executive branch has consistently defended the legality and efficacy of these surveillance programs.

This paper considers the nature and effect of the warrantless surveillance infrastructure constructed in the United States since the terrorist attacks of September 11, 2001, and discusses surveillance-related powers and accountability measures in the United Kingdom and India as comparative examples. Through this analysis, this paper questions whether accountability over government abuses in this area exist in an effective form, or if governments have constructed a post-9/11 legal architecture with regard to

* Professor of Law and Associate Dean for Faculty Development & Intellectual Life, Western New England University School of Law. The author is grateful for the comments offered on previous drafts of this paper, including those of participants at a forum of the Tilburg University Law and Economics Center in April 2014 and at the *Governing Intelligence* symposium hosted by the Stanford Journal of International Law in May 2014. The author thanks Julia Ballaschk, Matthew H. Charity, Elisebeth Collins Cook, Rajesh De, Federico Fabbrini, and J. Chris Inglis for their thoughtful comments and insights.

surveillance that engenders excessive secrecy and renders accountability mechanisms largely meaningless.

INTRODUCTION

What does it mean to maintain the rule of law, particularly when national security and counterterrorism policies are at issue? In its propagation of the "global war on terror" after the terrorist attacks of September 11, 2001, the Bush Administration was accused many times of behaving in a lawless fashion.[1] President Obama picked up on this theme, insisting early on that his administration would oversee a return to the primacy of the rule of law, regardless of whether the country viewed itself as being at peace or at war.[2] In doing so, Obama promised to restore the idea that the government should have limited power, should be held to account for its transgressions, and that the government's actions and the laws under which it acts ought to be transparent.[3]

Yet the post-9/11 decision-making by both the Bush and Obama administrations has been characterized by excessive secrecy that stymies most efforts to hold the government accountable for its abuses. Particularly in the area of government surveillance, meaningful oversight has seemed impossible without the trigger of leaked information. The executive branch has consistently defended the legality and efficacy of these surveillance programs, insisting that the administration acts in accordance with the rule of law and that secrecy has been necessary, and that leaks by government insiders have been criminal and counterproductive.[4] Congress has enabled the executive branch to engage in widespread surveillance in the post-9/11 context and has not been able to compel the executive branch to make available information regarding its surveillance programs that could give any oversight efforts more muscle.

This paper considers the nature and effect of national security-related surveillance and accountability measures constructed in the United States, the United Kingdom, and India since the terrorist attacks of September 11, 2001. In doing so, this paper questions whether accountability of government abuses in this area exist in a meaningful form, or if governments have constructed a post-9/11 legal architecture with regard to surveillance that engenders excessive secrecy in

---

[1] The Bush Administration's common response was that its practices and policies indeed comported with the law—its interpretation of the law. *See, e.g.*, Memorandum from the U.S. Dep't of Justice Office of Legal Counsel to Alberto R. Gonzales, Counsel to the President, Standards of Conduct for Interrogation Under 18 U.S.C. §§ 2340–2340A (Aug. 1, 2002) [hereinafter Bybee Memorandum] (defining "torture" narrowly for purposes of shielding U.S. interrogators from liability under international and domestic law). The administration likewise made efforts to amend the law to comport with its chosen path of action. *See, e.g.*, Adam Liptak, *Interrogation Methods Rejected by Military Win Bush's Support*, N.Y. TIMES (Sept. 8, 2006), http://www.nytimes.com/2006/09/08/washington/08legal.html?pagewanted=all&_r=0 (discussing ways in which the Bush administration sought to redefine lawlessness after adverse judicial decisions).

[2] *See* Barack Obama, Remarks by the President on Nat'l Sec. (May 21, 2009) [hereinafter 2009 National Archives Speech], http://www.whitehouse.gov/the-press-office/remarks-president-national-security-5-21-09.

[3] *See* Diane P. Wood, *The Rule of Law in Times of Stress*, 70 U. CHI. L. REV. 455 (2003) (defining one aspect of the rule of law as providing meaningful government constraint and accountability).

[4] *See* President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence (defending the legality and efficacy of NSA warrantless surveillance); David E. Sanger & John O'Neil, *White House Begins New Effort to Defend Surveillance Program*, WASH. POST (Jan. 23, 2006), http://www.nytimes.com/2006/01/23/politics/23cnd-wiretap.html?pagewanted=all&_r=0.

ways that render accountability mechanisms largely ersatz. Part I considers post-9/11 surveillance efforts in the United States and the legal architecture that has supported it. Part II questions whether the laws governing surveillance should legitimately be considered accountability mechanisms, or whether they instead mimic the rule of law by becoming relevant only when leaked information becomes available. Part III uses a comparative lens to consider the systems of surveillance adopted by the United Kingdom and India—other democratic nations struggling with security threats—and the efficacy of the accountability mechanisms in those nations. Part IV concludes with an exploration of possible avenues for the limitation of and accountability over government surveillance.

I. THE LEGAL ARCHITECTURE OF U.S. SURVEILLANCE EFFORTS

After the terrorist attacks of September 11, 2001, U.S. surveillance efforts were ramped up, in part due to the perception that intelligence agencies failed to garner vital information that could have prevented the attacks.[5] There was significant disagreement as to whether the failure was due primarily to legal constraints[6] or primarily to an inability to synthesize and analyze the available intelligence accurately and thoroughly.[7] The 9/11 Commission agreed with the latter view, concluding that the inability of intelligence agencies to learn about and prevent the attacks of September 11 was not attributable to a lack of legal authority.[8] Nonetheless, the legal and policy constraints on intelligence gathering were loosened significantly in the wake of the September 11 attacks. As discussed below, the PATRIOT Act arguably authorized the collection and storage of domestic telephony and internet metadata[9] and the collection and content searches

---

[5] *See* NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 339–60 (2004), *available at* http://www.9-11commission.gov [hereinafter 9/11 Commission Report] (discussing the inability of U.S. intelligence agencies to synthesize relevant data prior to the September 11th attacks).

[6] *See* Testimony of Attorney General John Ashcroft Before the National Commission on Terrorist Attacks Upon the United States 2 (Apr. 13, 2004), http://govinfo.library.unt.edu/911/hearings/hearing10/ashcroft_statement.pdf (noting that "[t]he single greatest structural cause for September 11 was the wall that segregated criminal investigators and intelligence agents. Government erected this wall. Government buttressed this wall. And before September 11, government was blinded by this wall").

[7] *See* Testimony of Professor Stephen J. Schulhofer Before the National Commission on Terrorist Attacks Upon the United States 1 (Dec. 8, 2003), *available at* http://govinfo.library.unt.edu/911/hearings/hearing6/witness_schulhofer.htm (noting that intelligence "capabilities are largely determined by non-legal constraints—technical, budgetary and human resources, the training and priorities of our officers and the organization and cultures of the relevant agencies—all areas where our deficits have been, and continue to be, enormous").

[8] *See* 9/11 Commission Report, *supra* note 5, at 339–60.

[9] The telephony metadata authorized for collection is defined as:

> [I]nclud[ing] comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station [sic] Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication . . . or the name, address, or financial information of a subscriber or customer.

See In re Application of the Fed. Bureau of Investigation 3 n.1 (FISA Ct. 2013), http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf.

of substantial amounts of foreign telephone and internet communications,[10] thereby giving the intelligence community a much larger "haystack" of information from which to attempt to glean details of emerging and ongoing terrorist threats.[11] This shift generated critiques from civil libertarians and lawmakers,[12] but critics have been largely unable to secure significant and lasting victories in curtailing surveillance powers, either through judicial action[13] or legislative initiative.

However, the tenor of the public debate became more contentious in June 2013, when then-National Security Agency (NSA) contractor Edward Snowden began revealing classified documents detailing the scope of NSA surveillance on foreign and U.S. persons in order to prompt public scrutiny and debate over the programs. Snowden revealed, among many other things, that the NSA was engaged in the practice of collecting and retaining the metadata of all U.S. telephone customers for five years (the "NSA Metadata Program"), and had been running searches through that metadata when there was a "reasonable, articulable suspicion" that a particular telephone number was associated with potential terrorist activity.[14]

This program—with its broad scope, lack of particularized suspicion, and lengthy duration of data retention—provides a useful vehicle through which to analyze the question of meaningful accountability over warrantless government surveillance more generally.[15] Snowden's revelations over the year following the publication of his initial disclosure continued to foster debate and demands for

---

[10] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107–56, § 215, 115 Stat. 287 [hereinafter PATRIOT Act] (arguably authorizing the collection and storage of bulk metadata); *id.* § 702 (authorizing the targeted collection of data, including content, from overseas targets). When various provisions of the Patriot Act were up for renewal in 2010, debates on the utility, invasiveness, and potential abuse of the surveillance provisions ended in congressional reauthorization of the Act without alternation. *See* David Kravets, *Lawmakers Punt Patriot Act to Obama*, WIRED (Feb. 26, 2010), http://www.wired.com/2010/02/lawmakers-renew-patriot-act/.

[11] *See* Gil Press, *The Effectiveness of Small vs. Big Data Is Where the NSA Debate Should Start*, FORBES (June 12, 2013), http://www.forbes.com/sites/gilpress/2013/06/12/the-effectiveness-of-small-vs-big-data-is-where-the-nsa-debate-should-start/ (discussing need to understand whether a larger or smaller "haystack" of data better enables intelligence-gathering and analysis efforts).

[12] *See, e.g.*, Felicia Sonmez, *Harry Reid, Rand Paul Spar over Patriot Act on Senate Floor*, WASH. POST (May 25, 2011), http://www.washingtonpost.com/blogs/2chambers/post/harry-reid-rand-paul-spar-over-patriot-act-on-senate-floor/2011/05/25/AGcgWRBH_blog.html (describing objections by Senators Rand Paul and Tom Udall to data-gathering provisions being debated for renewal as part of the Patriot Act).

[13] *E.g.*, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013) (holding that plaintiffs alleging unconstitutional and illegal surveillance lacked standing to bring their complaint because they had no publicly available proof of their surveillance). Cases that challenge these surveillance programs on constitutional and statutory grounds are still being litigated. *See infra* Part I.C.2 ("Article III Courts").

[14] *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[15] Of course, the U.S. intelligence community has engaged in numerous programs involving warrantless surveillance, and this paper only addresses the bulk metadata collection that is arguably authorized under Section 215 of the Patriot Act. Other warrantless surveillance—of non-U.S. persons or on non-U.S. territory—falls under the auspices of other authorities, such as Executive Order 12333 or Section 702 of the Foreign Intelligence Surveillance Act. Those surveillance and data collection efforts are beyond the scope of this paper. Nonetheless, the structural accountability questions raised with regard to the NSA Metadata Program can be extrapolated to consider other domestic surveillance questions because of analogous legal and political frameworks.

better oversight of the NSA.[16] The administration initiated various review mechanisms,[17] Congress convened oversight hearings,[18] and the public engaged in a vigorous debate as to the legality, efficacy, and morality of the NSA's activities, particularly the bulk collection and retention for several years of telephony and internet metadata of U.S. persons.

This collection has been described at times as lawless,[19] yet the architecture constructed to support arguments as to the domestic legality[20] and constitutionality of the NSA Metadata Program is extensive. On a purely constitutional level, some have asserted that inherent Article II power confers on the executive branch expansive surveillance powers based on a view that the United States continues to be on a post-9/11 war footing.[21] From a legislative perspective, a significant number of statutes, such as the Authorization for the Use of Military Force

---

[16] *See* James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for U.S. Citizens' Emails and Phone Calls*, GUARDIAN (Aug. 9, 2013), http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls; Michael Birnbaum & Ellen Nakashima, *German Leader Calls Obama About Alleged Cellphone Tapping*, WASH. POST (Oct. 23, 2013), http://www.washingtonpost.com/world/german-leader-calls-obama-about-alleged-cellphone-tapping/2013/10/23/2edb4aa2-3c10-11e3-b0e7-716179a2c2c7_story.html; James Risen & Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. TIMES (Sept. 28, 2013) http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all.

[17] *See infra*, Part II.A.

[18] *See infra,* Part II.B.

[19] *E.g.*, Glenn Greenwald, *An Ideology of Lawlessness*, UNCLAIMED TERRITORY (Jan. 6, 2006 9:07 AM), http://glenngreenwald.blogspot.com/2006/01/ideology-of-lawlessness.html (describing the Bush administration's telecommunications surveillance and data collection as indicative of the administration's general lawlessness with regard to its counterterrorism operations); Tori Mends-Cole, *Waterboarding Redux: Anthony Romero Takes on Yoo, Gonzales over Bush-Era "Lawlessness"*, ACLU (Aug. 3, 2011 9:07 AM), https://www.aclu.org/blog/human-rights-national-security/waterboarding-redux-anthony-romero-takes-yoo-gonzales-over-bush (discussing Bush-era detainee interrogation as "lawless").

[20] There are ongoing questions as to whether the practice of mass data collection, storage and mining by governments violates international legal standards, such as those articulated in the International Convention on Civil and Political Rights. *See, e.g.*, U.N. Secretary-General, *Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, U.N. Doc. A/69/397 (Sept. 23, 2014). The question of the NSA's international law compliance is beyond the scope of this project.

[21] *In re* Nat'l Sec. Agency Telecommunications Records Litig., 564 F. Supp. 2d 1109, 1116–17 (N.D. Cal. 2008) (describing the legality of NSA collection and retention of internet metadata based only on the president's authorization); U.S. DEP'T OF JUSTICE, THE NATIONAL SECURITY AGENCY PROGRAM TO DETECT AND PREVENT TERRORIST ATTACKS: MYTH VS. REALITY 1 (2006), *available at* http://www.justice.gov/opa/documents/nsa_myth_v_reality.pdf (arguing that the President's Commander in Chief authority under Article II put the Bush administration's Terrorist Surveillance Program on solid constitutional footing). *See generally* John C. Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 10 ISJLP 301 (2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2369192. In many respects, Professor Yoo's reliance on Article II authority to justify the constitutionality of surveillance programs mirrors the arguments made by the Bush administration justifying the indefinite detention of detainees at the Guantanamo Bay detention facility—see the government's claim in *Hamdi* as well as claims that Professor Yoo made while working in the Office of Legal Counsel on matters justifying the warrantless surveillance of domestic targets in wartime. *See* Memorandum from the U.S. Dep't of Justice Office of Legal Counsel to William J. Haynes II, Gen. Counsel of the Dep't of Def., Military Interrogation of Alien Unlawful Combatants Held Outside the U.S. 8 n.10 (Mar. 14, 2003) (referring back to an earlier, still-secret OLC memorandum entitled, "Authority for Use of Military Force to Combat Terrorist Activities within the United States").

(AUMF),[22] provisions of the USA PATRIOT Act (PATRIOT Act),[23] the Protect America Act and the FISA Amendments Act of 2008 (FAA)[24] were enacted by Congress and interpreted by the NSA as providing ample legal authority for the capture and storage of data.[25] Compounding these statutory authorities, the executive branch has likely sought its own nonpublic legal guidance in the form of secret legal opinions from the Office of Legal Counsel memoranda[26] and other Department of Justice memoranda defending the legality and efficacy of the surveillance program.[27]

The surveillance and data collection that are part of the NSA Metadata Program have been largely validated by two forms of relatively weak judicial review: Article III courts have, until recently, largely refused to hear the merits of cases challenging the government surveillance, instead finding that plaintiffs are unable to satisfy the standing requirement,[28] or dismissing suits at the pleadings stage due to invocations of the state secrets privilege by the government.[29] The Foreign Intelligence Surveillance Court (FISC), tasked with determining the legality of many of the government's surveillance requests, has largely acquiesced to the government's requests over the years.[30] Cases litigated after the Snowden revelations of June 2013 suggest, however, that the judicial deference offered to the government in many previous counterterrorism cases may be curtailed in light of public attention and critique of the NSA Metadata Program, as well as a

---

[22] *See* Authorization for the Use of Military Force (AUMF), Pub. L. No. 107-40, 115 Stat. 224 (2001).

[23] *See* Patriot Act, Pub. L. No. 107-56, § 218, 115 Stat. 287 (2001) (amending the Foreign Intelligence Surveillance Act of 1978 such that electronic surveillance and physical searches need only be justified in "significant" part by the goal of obtaining foreign intelligence); *Id.* at §§ 215, 702.

[24] *See* Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (amending Foreign Intelligence Surveillance Act of 1978 (FISA)); Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008). *See generally* AUMF; Patriot Act § 215.

[25] *See* Letter from Robert Weich, Assistant Att'y Gen., to Dianne Feinstein and Saxby Chambliss, Senate Select Committee on Intelligence Chair and Ranking Member (Feb. 2, 2011), *available at* http://www.dni.gov/files/documents/2011_CoverLetters_Report_Collection.pdf (discussing the legislative basis for the NSA bulk metadata collection program).

[26] *See* Michael J. Glennon, *National Security and Double Government*, 5 HARV. NAT'L SECURITY J. 1, 78 (2014) (describing the existence and possible content of such an Office of Legal Counsel memorandum); Dawn E. Johnson, *Faithfully Executing the Laws: Internal Legal Constraints on Executive Power*, 54 UCLA L. REV. 1559, 1577 (2007) (noting that OLC opinions are generally considered binding on the executive branch); *see also* Sudha Setty, *No More Secret Laws: How Transparency of Executive Branch Legal Policy Doesn't Let the Terrorists Win*, 57 U. KAN. L. REV. 579, 594–98 (2009) (detailing ways in which the Office of Legal Counsel has used secret law to justify and provide legal comfort to its operatives).

[27] *See* Weich, *supra* note 25 (including Justice Department analysis of the legislative authority supporting the NSA's bulk metadata collection program). Such memoranda, leaked to the public, have been used to justify other counterterrorism efforts, such as the Obama administration's use of extraterritorial drone strikes to kill suspected terrorists who are U.S. citizens. *See* DEP'T OF JUSTICE, LAWFULNESS OF A LETHAL OPERATION DIRECTED AGAINST A U.S. CITIZEN WHO IS A SENIOR OPERATIONAL LEADER OF AL-QA'IDA OR AN ASSOCIATED FORCE (2010), *available at* http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf.

[28] *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

[29] *See* Al-Haramain Islamic Found. v. Obama, 705 F.3d 845 (9th Cir. 2012).

[30] For example, in 2012 the FISC authorized every one of the 1, 788 government requests to conduct electronic surveillance that it was asked to rule on. *See* Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney General, to Senator Harry S. Reid (Apr. 30, 2013), *available at* http://fas.org/irp/agency/doj/fisa/2012rept.pdf.

reinvigorated judicial embrace of the privacy protections embodied in the Fourth Amendment.[31]

II. CURRENT MECHANISMS MIMIC THE ACCOUNTABILITY NECESSARY UNDER THE RULE OF LAW

NSA surveillance and data collection has been expansive during both the Bush and Obama administrations and has been supported by tremendous amounts of law constructed by the executive branch and Congress and construed by the courts to enable surveillance with little meaningful oversight. As such, we are left to question whether the legal architecture provides the constraints on government necessary to satisfy the basic tenets of the rule of law or, instead, if the legal architecture mimics and ultimately undermines efforts to uphold the rule of law.

Snowden's revelations with regard to a variety of surveillance activities, including the NSA Metadata Program, provoked anger from a wide and bipartisan swath of the U.S. public. This in turn forced the Obama administration, Congress, and the courts to respond as to the roles of the various branches of government in ensuring control and accountability over NSA surveillance. The Obama administration offered a multifaceted response: defending the efficacy, legality and necessity of the NSA Metadata Program,[32] claiming that current accountability mechanisms were adequate,[33] and ordering reviews that allowed for the possibility of curtailing and/or creating additional accountability safeguards over aspects of the NSA Metadata Program.[34] Members of Congress varied in their reactions with regard to the NSA Metadata Program: some defended the legality, necessity and efficacy of the program,[35] while others were energized by the public disclosure to push for additional safeguards for civil liberties.[36] The FISC, normally insulated from public view, came under scrutiny as the judicial entity tasked with safeguarding civil liberties. As such, FISC judges were put on the defensive as to whether or not their decisions effectively prevented or curtailed unlawful or unconstitutional surveillance and, thereby, genuinely upheld the rule of law.

---

[31] *See, e.g.*, Klayman v. Obama, F. Supp. 2d 1 (D.D.C. 2013) (finding that the Section 215 metadata collection program is illegal and possibly unconstitutional based on Fourth Amendment concerns); *see also* Riley v. California, 134 S.Ct. 2473, 2429 (2014) (holding that a warrantless search of an arrested individual's cell phone contents violated the Fourth Amendment).

[32] *See* Barack Obama, *Remarks by the President in a Press Conference*, WHITE HOUSE (Aug. 9, 2013), http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference [hereinafter *August 2013 Remarks by the President*].

[33] *See id.*

[34] *See id.*

[35] *See* Editorial, *President Obama's Dragnet*, N.Y. TIMES (June 7, 2013), http://www.nytimes.com/2013/06/07/opinion/president-obamas-dragnet.html?pagewanted=all (describing the defense of NSA bulk data collection offered by Senate Intelligence Committee Chair Dianne Feinstein and Ranking Member Saxby Chambliss).

[36] *See* Robert Barnes, Timothy B. Lee & Ellen Nakashima, *Government Surveillance Programs Renew Debate About Oversight*, WASH. POST (June 8, 2013), http://www.washingtonpost.com/politics/government-surveillance-programs-renew-debate-about-oversight/2013/06/08/7f5e6dc4-d06d-11e2-8f6b-67f40e176f03_story.html (including comments by staffers to Senator Ron Wyden regarding the strict limitations on access to information regarding surveillance programs for members of the Senate Intelligence Committee).

A. Administration Claims of Accountability

In the months after the Snowden leaks in 2013, the Obama administration sought to emphasize several aspects of the NSA's work with regard to the public debate: the danger that transparency could compromise the utility of the NSA's surveillance efforts;[37] the efficacy of the NSA Metadata Program in securing intelligence essential to detect and disrupt terrorist threats;[38] and the fact that there had been very few abuses of the power granted to the NSA.[39]

The administration insisted that it had shared a relatively full account of the NSA Metadata Program with Congress prior to Congress's reauthorization of the PATRIOT Act in 2011,[40] underscoring its claim that the NSA was not acting as a rogue agency. The level of actual congressional knowledge as to the scope and depth of the program remains unclear. In August 2013, various members of Congress from both major political parties attested that they had never been given the information at issue and had voted on PATRIOT Act renewal without a satisfactory understanding of the NSA surveillance program, arguably because the heads of intelligence committees in Congress had chosen not to share that information with members not serving on those panels.[41] On the other hand, it was likely a matter of political self-interest for members of Congress to deny knowledge

---

[37] *See, e.g.*, Josh Gerstein, *Obama Aides: Transparency Plans Could Harm Security*, POLITICO (Nov. 13, 2013 1:39 PM), http://politi.co/185oWve. This claim echoed those made by the Bush administration when the question of warrantless wiretapping and the complicity of telecommunications companies arose in 2007 and 2008. *See Oversight of the U.S. Dep't of Justice Hearing Before the Senate Judiciary Comm.*, 110th Cong. 7, 13–14 (2008), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110shrg52691/pdf/CHRG-110shrg52691.pdf (providing the statement of Attorney General Michael Mukasey, who refused to testify as to the role of telecommunications companies in the government's warrantless surveillance program on the grounds that to do so would compromise national security interests by publicizing the "means and methods" used by the administration). The secrecy surrounding these programs makes evidence-based oversight and accountability measures extremely difficult if not impossible. *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 17–18 (2008). The diffusion of responsibility within the national security bureaucracy, combined with the lack of transparency of action, also contributes to a structural inability to hold responsible individuals accountable for abuses of power. *See* PAUL C. LIGHT, THICKENING GOVERNMENT: FEDERAL HIERARCHY AND THE DIFFUSION OF ACCOUNTABILITY 62, 86–87 (1994).

[38] *See August 2013 Remarks by the President*, *supra* note 32. During this press conference, President Obama noted the efficacy of the surveillance programs arguably authorized under various sections of the Patriot Act and the Foreign Intelligence Surveillance Act: "[M]y determination was that the two programs in particular that had been an issue—215 and 702—offered valuable intelligence that helps us protect the American people, and they're worth preserving"); *see also* Glennon, *supra* note 26, at 26-27, 29 (discussing the structural incentives for national security administrators to exaggerate the nature and scope of threats to U.S. security).

[39] *See August 2013 Remarks by the President*, *supra* note 32. President Obama insisted that the surveillance programs were not being abused and were being adequately overseen by the Foreign Intelligence Surveillance Court ("What you're hearing about is the prospect that these could be abused. Now part of the reason they're not abused is because they're—these checks are in place, and those abuses would be against the law and would be against the orders of the FISC").

[40] *See* Weich, *supra* note 25 (outlining the bulk data collection conducted by the government pursuant to Section 215 of the Patriot Act and with the permission of the FISA court).

[41] *See* Spencer Ackerman, *Intelligence Committee Withheld Key File Before Critical NSA Vote, Amash Claims*, GUARDIAN (Aug. 12, 2013, 5:37 PM), http://www.theguardian.com/world/2013/aug/12/intelligence-committee-nsa-vote-justin-amash (noting that congressional leaders had not shared the relevant information with their colleagues prior to voting for Patriot Act reauthorization).

of a program of which they had a general understanding, but was deeply unpopular with much of the public after the Snowden disclosures.

As the disclosures and public critique continued, the Obama administration promised to increase accountability and transparency of the NSA Metadata Program, first by announcing the creation of the Review Group on Intelligence and Communications Technologies. This program was established by Director of National Intelligence James Clapper.[42] The announcement expressed the purpose of the review group as assessing whether surveillance technology was being used in a way that optimized national security and the advancement of U.S. foreign policy interests, "while appropriately accounting for other policy considerations, such as the risk of unauthorized disclosure and our need to maintain the public trust."[43] The Review Group issued a lengthy report in December 2013 that focused on proactive suggestions, among them that the bulk collection and storage of metadata ought to remain in the possession of an entity outside of the government, that the statutory framework under the PATRIOT Act Section 215 be amended to require FISC authorization for the NSA to conduct searches within the bulk metadata, that more information regarding intelligence gathering should be disclosed to Congress and the public, that more consistent and rigorous accountability measures ought to be implemented, and that non-U.S. persons ought to be afforded more protection from potential U.S. government overreach.[44]

In January 2014, President Obama, citing the need for continued oversight of intelligence agencies while defending the need for bulk data collection and for the secrecy surrounding that program, announced that various aspects of the NSA Metadata Program and other intelligence gathering initiatives would change to improve privacy safeguards for U.S. and non-U.S. persons.[45] President Obama further stated that a number of FISC opinions would be declassified and made public, and that transparency would become a priority for intelligence agencies.[46] Shortly after this speech, the Privacy and Civil Liberties Oversight Board, an independent body within the executive branch whose establishment was recommended by the 9/11 Commission, issued a detailed report in which it concluded that the PATRIOT Act did not provide a statutory basis for the bulk collection and retention of telephony metadata, that the NSA Metadata Program raised constitutional concerns, and that it could find no significant evidence in

---

[42] *See* James R. Clapper, *DNI Clapper Announces Review Group on Intelligence and Communications Technologies*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE (Aug. 12, 2013), http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/909-dni-clapper-announces-review-group-on-intelligence-and-communications-technologies.

[43] *Id.* Nowhere in this announcement were individual privacy, civil liberties, and constitutional rights addressed.

[44] *See* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 17–21 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[45] Barack Obama, *Remarks by the President on Review of Signals Intelligence*, WHITE HOUSE (Jan. 17, 2014, 11:15 AM), http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [hereinafter *January 2014 Remarks by the President*].

[46] *Id.*

support of the efficacy of the program in disrupting and preventing terrorism threats.[47]

In late March 2014, the Obama administration announced that it would propose legislation to dismantle the bulk collection program, leaving metadata in the exclusive possession of telecommunications companies and requiring FISC authorization prior to the NSA accessing the metadata.[48] The type and scope of legislative restrictions were debated extensively in 2014, but no bill was passed, leaving open the question of whether any additional legislative control will be exerted by Congress—if not, the status quo of executive control over the scope and intrusiveness of the program will continue.[49] Section 215 of the Patriot Act, arguably providing statutory authorization of the NSA Metadata Program, is set to expire in July 2015, a deadline that is sure to prompt legislative debate on whether to renew the program, curtail the authority granted to the administration, or eliminate the program altogether. The effect of any legislation in curtailing intrusive surveillance practices is yet to be seen, but the fact that the administration has already shifted its public willingness to improving protections of privacy and civil liberties and increase transparency when compatible with intelligence gathering interests, is noteworthy as well.[50] Assessment of whether those changes will be meaningful must wait for further developments, particularly as it may be institutionally and politically difficult for the president and Congress to shift course dramatically in the face of still-existing terrorist threats and the political pressure created by the public perception of those threats.[51]

The primary message from the Obama administration since the Snowden disclosures has been that the administration itself is best suited to address whether and to what extent any recommended changes to NSA surveillance were appropriate,[52] and that the Snowden disclosures themselves have been unnecessary,

---

[47] PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 10–11 (2014), *available at* http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program-2.pdf.

[48] *See* Charlie Savage, *Obama to Call for End to N.S.A.'s Bulk Data Collection*, N.Y. TIMES (March 24, 2014), http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html.

[49] From late 2013 through 2014, Congress debated and amended the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection and Online Monitoring Act (USA Freedom Act), intended to curtail the bulk metadata collection program under Section 215 of the Patriot Act. The bill was passed in the House of Representatives, but did not pass in the Senate. *See* USA Freedom Act, H.R.3361, 113th Cong (2013), *available at* https://beta.congress.gov/bill/113th-congress/house-bill/3361.

[50] *See* Barack Obama, *Remarks by the President at the United States Military Academy Commencement Ceremony*, WHITE HOUSE (May 28, 2014, 10:22 AM), available at http://www.whitehouse.gov/the-press-office/2014/05/28/remarks-president-west-point-academy-commencement-ceremony ("Our intelligence community has done outstanding work, and we have to continue to protect sources and methods. But when we cannot explain our efforts clearly and publicly, we face terrorist propaganda and international suspicion, we erode legitimacy with our partners and our people, and we reduce accountability in our own government."); *see also id.* ("[W]e're putting in place new restrictions on how America collects and uses intelligence—because we will have fewer partners and be less effective if a perception takes hold that we're conducting surveillance against ordinary citizens.").

[51] *See* Sudha Setty, *National Security Interest Convergence*, 4 HARV. NAT'L SEC. J. 185, 188–189 (2012) (highlighting the political danger of being viewed as "soft on terror"); *see also* Glennon, *supra* note 26, at 66 (asserting that presidents rarely change course dramatically in the arena of foreign affairs because of the deep entrenchment of beliefs and positions among experts and policy makers).

[52] *See* Glennon, *supra* note 26, at 40.

illegal, and counterproductive to both the intelligence gathering programs themselves and the public discourse.[53] However, there is no indication that any of the accountability measures now being promoted by the administration would have existed or gained significant purchase but for the Snowden public disclosures.[54] The various institutional accountability mechanisms that currently exist within the executive branch do not appear to be equipped to consider concerns stemming from intelligence community insiders who have a fuller understanding than the public of the scope and nature of surveillance programs and who question the basic premise or constitutionality of programs such as the NSA metadata collection. To the contrary, there are indications that some within the NSA have actively attempted to avoid oversight by the Department of Justice.[55] The Office of the Inspector General for the NSA, appointed by and reporting to the director of the NSA,[56] is suited to deal with allegations of statutory and policy compliance violations, but not with a large scale systemic complaint about privacy and accountability such as that of Snowden.[57] Other potential avenues for accountability, such as the Office of the Inspector General for the Defense Department, are rendered irrelevant by the lack of information access.[58] In fact, the extreme secrecy that surrounded these surveillance programs, even within the administration, suggests that many existing executive branch mechanisms were, in the time before the Snowden disclosures, not engaged in effective oversight.

---

[53] *See, e.g.*, *January 2014 Remarks by the President*, *supra* note 45.

[54] Snowden provided written testimony to the European Parliament stating that he had attempted to discuss his concerns with regard to various aspects of NSA surveillance with superiors within the NSA prior to his public disclosure, but that his efforts were either ignored or rebuffed. *See* Edward J. Snowden, *Answers to Written Questions From the European Parliament*, EUR. PARL. 1, 5 (March 7, 2014), http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf.

[55] *See* Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, WASH. POST (Aug. 15, 2007), 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 (stating that NSA operatives requesting permission to extend surveillance to a new target were instructed to limit the information disclosed to Justice Department "overseers").

[56] Commentators have suggested that an independently appointed and overseen Inspector General for the NSA would provide a better avenue for accountability. *See* Britt Snider & Charles Battaglia, *The National Security Agency Needs an Independent Inspector General*, WASH. POST (Sept. 26, 2013), http://www.washingtonpost.com/opinions/national-security-agency-needs-an-independent-inspector-general/2013/09/26/ae37d7fc-25f4-11e3-ad0d-b7c8d2a594b9_story.html.

[57] *See* Interviews with NSA officials (various dates, on file with author) (discussing the fact that the job of the NSA Inspector General would not have been to discuss the "philosophical differences" that Snowden had with the NSA's programmatic and policy choices). The Inspector General for the NSA has publicly stated that if Snowden had complained to the Inspector General, his allegations would have been investigated thoroughly. Darren Samuelsohn, *NSA Watchdog: Snowden Should Have Come to Me*, POLITICO (Feb. 25, 2014, 6:37 PM) http://politi.co/NvvjAE. But it seems quite likely that the extent of the Inspector General's inquiry would have been to examine the program against the existing statutory authority and find that the bulk data collection was statutorily authorized.

[58] *See* Spencer Ackerman, *Pentagon Watchdog 'Not Aware' of NSA Bulk Phone Data Collection*, GUARDIAN (Mar. 18, 2014, 3:36 PM), http://www.theguardian.com/world/2014/mar/18/pentagon-watchdog-nsa-bulk-phone-collection (stating that the Defense Department Deputy Inspector General was unaware of the bulk data collection until learning about it through the June 2013 Snowden leaks).

B. Congressional Efforts at Oversight and Accountability Enforcement

The extent of congressional knowledge regarding the NSA Metadata Program is not fully known to the public and has been the subject of significant debate. Nonetheless, even assuming that Congress was sufficiently informed as to the potential reach of the PATRIOT Act with regard to surveillance[59] and, therefore, that the statutory authority for the bulk data collection and storage was sound, the ability of Congress to effect significant and meaningful ex post oversight appears to be severely limited.

Historically, congressional hearings and investigations have been a powerful tool to rein in executive branch overreaching.[60] However, it seems that the extreme secrecy surrounding the NSA surveillance programs undermined the efficacy of these oversight powers, to the point that they may have been reduced to an ersatz form of accountability. One prominent example stems from a Senate oversight hearing on March 12, 2013, in which Senator Ron Wyden specifically asked Director of National Intelligence James Clapper if the NSA was systematically gathering information on the communications of millions of Americans.[61] Clapper denied this, yet subsequent revelations confirmed that the broad scope of the data collection included metadata for telephonic communications, as well as content data for emails, texts, and other such writings.[62] After public discussion of the discrepancy in his testimony, Clapper commented that he gave the "least most untruthful" answer possible under the circumstances.[63] Senator Wyden expressed disappointment and frustration that even while under oath at an oversight hearing, Clapper misled the Senate.[64]

The ability for congressional oversight is further hampered by a general lack of access to information about the details of the NSA Metadata Program [65] and

---

[59] *See* Weich, *supra* note 25 (discussing the need for Congress to be sufficiently informed such that it could renew Section 215 of the Patriot Act in 2011).

[60] *See, e.g.*, McGrain v. Daugherty, 273 U.S. 131, 161 (1927) (noting that the power of legislative inquiry has been long established in the United States).

[61] Senator Wyden posed the following question: "[D]oes the NSA collect any type of data at all on millions or hundreds of millions of Americans?" Clapper responded, "*[n]*o, sir." *See* Glenn Kessler, *James Clapper's "Least Untruthful" Statement to the Senate*, WASH. POST (June 12, 2013, 6:00 AM), http://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html.

[62] *See* Siobhan Gorman & Jennifer Valentino-Devries, *New Details Show Broader NSA Surveillance Reach*, WALL ST. J. (Aug. 20, 2013, 11:31 PM), http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html (describing how 75% of email traffic, including the content of emails, sent or received by United States persons is captured by various NSA programs).

[63] *See* James R. Clapper, *Director James R. Clapper Interview with Andrea Mitchell*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE (June 8, 2013, 1:00 PM), http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/874-director-james-r-clapper-interview-with-andrea-mitchell.

[64] *See* Aaron Blake, *Sen. Wyden: Clapper Didn't Give 'Straight Answer' on NSA programs*, WASH. POST (June 11, 2013), http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/11/sen-wyden-clapper-didnt-give-straight-answer-on-nsa-programs.

[65] *See* Weich, *supra* note 25 (detailing the limitations on sharing information with staffers, taking notes, or retaining any written record of the information that members of congressional oversight access with regard to the NSA bulk metadata collection program).

lack of ability to discuss publicly whatever knowledge is shared with Congress.[66] In fact, it remains unclear whether senators, including Dianne Feinstein, Chair of the Senate Intelligence Committee, knew of the lapses in NSA procedure until after such information was leaked to news sources.[67] Further revelations indicate that administration statements made to Congress even after the Snowden disclosures were not entirely accurate.[68] These examples are not determinative, but taken together, they raise significant doubt to the extent of accurate information regarding surveillance programs being made available to congressional oversight committees, and whether the oversight committees can function as effective accountability measures[69] without the benefit of illegally leaked information such as the Snowden disclosures.

C. Judicial Review

Two forms of relatively weak judicial review exist over the NSA Metadata Program. The primary mechanism by which the NSA has legitimated its surveillance activities is the Foreign Intelligence Surveillance Court (FISC), a closed, non-adversarial setting. Article III courts have had the opportunity to consider post-9/11 surveillance programs on numerous occasions, and with few exceptions, Article III courts have refused to review matters of national security-related surveillance.

1. Foreign Intelligence Surveillance Court

The FISC differs from Article III courts in numerous ways: Its statutory scope is limited to matters of foreign intelligence gathering; its judges are appointed in the sole discretion of the Chief Justice of the United States Supreme Court; its proceedings are secret; its opinions are often secret or are published in heavily

---

[66] *See* Senator Ron Wyden & Senator Mark Udall, *Wyden, Udall Statement on Reports of Compliance Violations Made Under NSA Collection Programs*, RON WYDEN SENATOR FOR OR. (Aug. 16, 2013), http://www.wyden.senate.gov/news/press-releases/wyden-udall-statement-on-reports-of-compliance-violations-made-under-nsa-collection-programs (noting that the disclosures of thousands of violations by the NSA are "just the tip of a larger iceberg" and that they are prohibited from discussing the further problematic aspects of the NSA surveillance program by Senate rules).

[67] *See* Gellman, *supra* note 55 (noting that Senator Feinstein only learned of the audit from the Washington Post).

[68] *See NSA Report on Privacy Violations in the First Quarter of 2012*, WASH. POST (last visited Mar. 1, 2015), *available at* http://apps.washingtonpost.com/g/page/national/nsa-report-on-privacy-violations-in-the-first-quarter-of-2012/395/; Gellman, *supra* note 55 (providing and detailing the audit that found 2,276 violations of the NSA's own rules in several surveillance locations); *see also* Ellen Nakashima, *Lawmakers, Privacy Advocates Call for Reforms at NSA*, WASH. POST (Aug. 16, 2013), http://www.washingtonpost.com/world/national-security/lawmakers-privacy-advocates-call-for-reforms-at-nsa/2013/08/16/7cccb772-0692-11e3-a07f-49ddc7417125_story.html (stating that the White House emphasized that although there were a small number of "willful" transgressions, most were unintentional).

[69] Senator Dianne Feinstein's March 2014 allegations that the Central Intelligence Agency was conducting illegal and unconstitutional surveillance of communications among her staff members reinforced the perception that the surveillance apparatus of the administration was beyond the ability of Congress to effect meaningful oversight. *See* Mark Mazzetti, *Computer Searches at Center of Dispute on CIA Allegations*, N.Y. TIMES (Mar. 5, 2014), http://nyti.ms/1q95eGD (detailing allegations of CIA surveillance of Senate investigative work regarding Bush-era interrogation practices).

redacted form; and its process is not adversarial as only government lawyers make arguments defending the legality of the surveillance being contemplated.[70] Many of these differences bring into doubt the legitimacy of the court, its ability to afford adequate due process regarding civil liberties concerns, and its ability to uphold the rule of law in terms of government accountability. Compounding this legitimacy deficit is the FISC's own loosening of the relevance standard under Section 215 of the PATRIOT Act such that the FISC has found that bulk data collection without any particularized threat or connection to terrorism is legally permissible.[71]

Historically, the FISC has rejected NSA surveillance applications too infrequently to be considered a substantial check on government overreach as an ex ante matter.[72] As an ex post matter, it is unclear to what extent the FISC's work guarantees any meaningful accountability over NSA surveillance activities. On the one hand, because the FISC lacks an adversarial process and has no independent investigatory authority, the FISC only addresses ex post compliance problems when the government itself brings the problem to the court's attention.[73] As such, FISC judges rely on the statements of the government as to the government's own behavior and lack the authority to investigate the veracity of the government's representations.[74] For example, in 2011, the FISC found one aspect of the surveillance program—brought to its attention months after the program went into effect[75]—to be unconstitutional.[76] Additionally, in one declassified opinion, the FISC critiques the NSA's sloppy over-collection of metadata of U.S. communications, and questions the efficacy of bulk data collection as a national security measure.[77] At one point, the FISC sanctioned the NSA for overreaching in

---

[70] *See* Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1861 (2012); *see generally* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757 (2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2344774 (describing the process by which the FISC determines whether surveillance is legal).

[71] *See* Jennifer Valentino-Devries & Siobhan Gorman, *Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering*, WALL ST. J. (July 8, 2013), http://online.wsj.com/news/articles/SB10001424127887323873904578571893758853344.

[72] Between 1979 and 2012, the FISC received over 30,000 surveillance applications from the government and rejected fewer than 0.1% of them. *See Foreign Intelligence Surveillance Act Court Orders 1979–2012*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/wiretap/stats/fisa_stats.html (last updated May 1, 2014).

[73] *See In re* Prod. of Tangible Things from Redacted, No. BR 08-13, 2009 WL 9150913 (Foreign Intel. Surv. Ct. Mar. 2, 2009) (reprimanding NSA for the non-compliance with FISC orders).

[74] *See* Carol D. Leonnig, *Court: Ability to Police U.S. Spying Program Is Limited*, WASH. POST (Aug. 15, 2013), http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html (citing U.S. district judge Reggie Walton and noting that "the court lacks the tools to independently verify how often the government's surveillance breaks the court's rules . . . [and] it also cannot check the veracity of the government's assertions that the violations its staff members report are unintentional mistakes").

[75] *See* Gellman, *supra* note 55 (noting that the FISC decision was issued in October 2011, months after the program had been initiated).

[76] *See First Direct Evidence of Illegal Surveillance Found by the FISA Court*, WASH. POST (Oct. 12, 2011), *available at* http://apps.washingtonpost.com/g/page/national/first-direct-evidence-of-illegal-surveillance-found-by-the-fisa-court/393/ (noting an October 3, 2011 decision by FISC invalidating certain aspects of the NSA's surveillance programs).

[77] *See Judge's Opinion on N.S.A. Program*, N.Y. TIMES 5 (Aug. 22, 2013), http://www.nytimes.com/interactive/2013/08/22/us/22nsa-opinion-document.html (discussing the fact that some of the searches being run by the NSA were "wholly unrelated" to the stated purpose of those searches and that it was unclear whether the government's efforts to protect against unrelated searches were effective); *see also* Charlie Savage & Scott Shane, *Secret Court Rebuked N.S.A. on Surveillance*,

saving all metadata and running daily metadata against an "alert list" of approximately 17,800 phone numbers, only 10% of which had met FISC's legal standard for reasonable suspicion.[78] On such occasions, the administration has modified problematic aspects of the surveillance and continued forward without further impediment by the FISC.[79]

On the other hand, the fact that the NSA itself has brought potential compliance incidents to the notice of the FISC[80] indicates at least some internal policing of these programs. However, this is hardly an effective substitute for external review and accountability mechanisms that would ensure that consistent controls are in place. Further, the self-reporting of these compliance incidents does not in any way allow for discourse over the larger structural questions surrounding the surveillance programs.

Finally, the ability of the FISC to act as an effective check on NSA overreaching is severely limited by the secrecy and lack of information available to the FISC judges. Judge Reggie B. Walton, formerly the Chief Judge of the FISC, lamented that "[t]he FISC is forced to rely upon the accuracy of the information that is provided to the Court . . . . The FISC does not have the capacity to investigate issues of noncompliance . . . ."[81] The ability of the NSA to not only gather and retain bulk metadata, but also to build in backdoor access into data files despite private encryption efforts has been largely sanctioned by the FISC based on NSA representations as to the seriousness of the security threats posed to the nation.[82] In an environment in which there is a tremendous fear of being held responsible for any future terrorist attack that might occur on U.S. soil,[83] and in which there is a

---

N.Y. TIMES (Aug. 22, 2013), http://www.nytimes.com/2013/08/22/us/2011-ruling-found-an-nsa-program-unconstitutional.html?pagewanted=all (detailing the various ways in which the court found the NSA's surveillance to be unconstitutional).

[78] *See* Scott Shane, *Court Upbraided N.S.A. on Its Use of Call-Log Data*, N.Y. TIMES (Sept. 11, 2013), http://www.nytimes.com/2013/09/11/us/court-upbraided-nsa-on-its-use-of-call-log-data.html?pagewanted=all (noting that the FISC issued a "sharply worded" ruling in March 2009 describing the NSA's failure to comport with the limits set by the FISC and noting that the NSA had deliberately misled the FISC).

[79] *See* Barton Gellman, *NSA Statements to the Post*, WASH. POST (Aug. 15, 2013), http://www.washingtonpost.com/world/national-security/nsa-statements-to-the-post/2013/08/15/f40dd2c4-05d6-11e3-a07f-49ddc7417125_story.html (clarifying the effect of the FISC decision and noting that the surveillance program was modified such that it could continue with the approval of the FISC).

[80] *In re* Prod. of Tangible Things from Redacted, No. BR 08-13, 2009 WL 9150913 at *5 (Foreign Intel. Surv. Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2026%202009%20Notification%20of%20Compliance%20Incident.pdf (including NSA admission that the handling of metadata did not comply with the FISC's previous orders and outlining a plan to remedy the situation).

[81] *See* Carol Leonnig, *Court: Ability to Police U.S. Spying Program Limited*, WASH. POST (Aug. 15, 2013), http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html (quoting Judge Walton's written comments to the Washington Post).

[82] *See* Nicole Perlroth, Jeff Larson & Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES (Sept. 6, 2013), http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all (discussing NSA efforts to make encryption software vulnerable, and noting that much of this activity has been sanctioned by the FISC).

[83] *Transcript of President Obama's Jan. 17 Speech on NSA Reforms*, WASH. POST (Jan 17, 2014), http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html (noting that the NSA worked under the concern that if another terrorist attack occurred, the NSA might be held responsible, President

information deficit for those outside of the intelligence community, the FISC has consistently deferred to the NSA's assertions and has not been able to act as an effective accountability mechanism.

2. *Article III Courts*

Article III courts have consistently been wary of wading into the debate over surveillance, almost always dismissing cases in the post-9/11 context on procedural or secrecy grounds,[84] despite[85] the net effect of precluding even those individuals with concrete evidence that their privacy and civil liberties had been infringed from having their grievances heard.[86] Although the Snowden disclosures have given more purchase to plaintiffs challenging data collection and surveillance, some Article III courts continue to find that plaintiffs have no grounds to stop the NSA's data and metadata collection, retention, and analysis.

The case of *Clapper v. Amnesty International*,[87] decided in early 2013, prior to the Snowden disclosures, exemplifies the traditional lack of relief available to plaintiffs in Article III courts. In *Clapper*, plaintiffs, including attorneys, non-profit humanitarian organizations, and journalists, alleged that their ability to communicate with and advise overseas clients and sources was severely compromised by the fact that their phone calls were likely being surveilled by the NSA or other U.S. government agencies. The United States Supreme Court dismissed plaintiffs' suit on standing grounds, holding that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[88]

Immediately after Snowden's June 2013 disclosures that the telephony data of all U.S. persons is being systematically collected and stored by the NSA, the ability of plaintiffs to clear the procedural hurdle of standing improved, since the "fears of hypothetical future harm" that allowed the *Clapper* majority to dismiss that case were no longer hypothetical, but publicly known as fact. However, the question of whether plaintiffs were granted any substantive relief is yet to be determined, since district courts have come to differing conclusions on the question of the metadata collection program's constitutionality.

Obama mentioned this pressure overtly; it is certainly plausible that the members of the FISC view themselves under similar pressure).

[84] *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013) [hereinafter Clapper I] (dismissing suit alleging unconstitutional and unlawful surveillance based on standing grounds); Al-Haramain Islamic Found., Inc. v. Obama, 690 F.3d 1089 (9th Cir. 2012) (reversing lower court decision and dismissing suit that alleged unlawful government surveillance based on government invocation of the state secrets privilege).

[85] Some commentators suggest that courts are deliberate in their efforts to prevent rigorous examination of national security policies as a means of entrenching power in the national security policymakers. *See* Glennon, *supra* note 26, at 47–52.

[86] *See* Sudha Setty, *Judicial Formalism and the State Secrets Privilege*, 38 WM. MITCHELL L. REV. 1629, 1651–52 (2012) (arguing that U.S. courts need to engage affirmatively in the adjudication of national security litigation).

[87] *See* Clapper I.

[88] *See Cla*pper I at *2.

In *American Civil Liberties Union v. Clapper* ("*Clapper II*"), filed days after the initial Snowden disclosures,[89] the ACLU and other organizations claimed that the NSA's metadata collection and retention program violated their First and Fourth amendment rights by inhibiting their ability to speak freely with clients and by unreasonably searching and seizing their communications.[90] Judge Pauley of the Southern District of New York rejected these claims, holding that although the metadata "[i]f plumbed . . . can reveal a rich profile of every individual,"[91] under the long-standing precedent of *Smith v. Maryland*,[92] plaintiffs had no reasonable expectation of privacy over their telephony metadata. Further, Judge Pauley accepted the government's position that the metadata was necessary in disrupting several terrorist threats, and that such counterterrorism work could not have occurred without the vast trove of data available through the NSA Metadata Program.[93]

With similar facts and claims,[94] Judge Leon of the District Court of the District of Columbia in *Klayman v. Obama* differed from the *Clapper II* court and concluded that the constitutionality, statutory authority and efficacy of the NSA's bulk metadata collection program is, at best, questionable.[95] Judge Leon used these distinctions of both scope and depth of surveillance to establish that the NSA metadata program constituted a search for Fourth Amendment purposes.[96] In a particularly remarkable analysis, Judge Leon reasoned that the continuously expanding use of technology in the everyday lives of most Americans justified a greater expectation of privacy over information that is shared electronically, not an ever-shrinking realm of protection over personal privacy.[97]

Having established that a search occurred, Judge Leon considered the plaintiffs' request for preliminary injunctive relief, finding that there was a

---

[89] *See* Complaint for Declaratory and Injunctive Relief, ACLU v. Clapper, No. 13-3994 (S.D.N.Y. June 11, 2013) [hereinafter Clapper II], *available at* https://www.aclu.org/files/assets/nsa_phone_spying_complaint.pdf.

[90] *See* Clapper II.

[91] *See id.* at *2.

[92] *Id.* at *39–40 (citing Smith v. Maryland, 442 U.S. 735 (1979)) (holding that plaintiff had no reasonable expectation of privacy over telephone metadata, such as the telephone numbers of calls dialed from or received by his home telephone, since that information had been voluntarily shared with a third party, the telephone company).

[93] *See id.* at *35. The court further rejected plaintiffs' First Amendment claim on both standing and substantive grounds, holding that any chilling effect on plaintiffs' communications was based on their own "speculative fear" that their data was being reviewed by the NSA, not simply collected like that of every other U.S. person. *See id.* at *46–47.

[94] Plaintiffs alleged violations of the First, Fourth and Fifth Amendments, as well as statutory violations. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 9 (D.D.C. 2013).

[95] *Id.* at 5–6 (granting, but staying, a preliminary injunction based on the likelihood that plaintiffs would prevail on statutory and constitutional grounds).

[96] *Id.* at 44–45. Judge Leon framed the questions as, "When do present-day circumstances—the evolutions in the Government's surveillance capabilities citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer . . . is now." *Id.* at 45. Judge Leon took careful note of the Government's "almost Orwellian" surveillance capabilities, which informed his analysis of what constitutes a search. *Id.* at 49–50.

[97] *Id.* at 54–55. This analysis reflects the thinking of Justice Marshall in his *Smith v. Maryland* dissent, in which he opined that "unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance." 442 U.S. at 750 (referring to the government's argument that by using his home telephone, Smith had assumed the risk of government surveillance) (internal citations omitted).

significant likelihood that the plaintiffs would succeed in demonstrating that the surveillance and searches were unreasonable and, therefore, unconstitutional. To do so, he touched upon the intrusive nature of the search and, differing significantly from Judge Pauley in *Clapper II*, found that the government had not made a showing that the NSA Metadata Program was necessary to the government's counterterrorism efforts.[98]

Klayman offers some reason for optimism among civil libertarians: Not only did an Article III court decide a post-9/11 abuse of power case on its merits, but that decision held that the NSA surveillance at issue was likely in violation of the Fourth Amendment. Whether appellate courts will follow the line of reasoning in *Klayman* as opposed to that of *Clapper II* and *Smith*, however, remains unclear.[99] It is also difficult to predict how the U.S. Supreme Court will respond when confronted with this matter. On the one hand, individual members of the Court have expressed skepticism as to the appropriateness of judicial review in matters of national security-related surveillance.[100] On the other, the Court as a whole has recently shown significant interest in rethinking the parameters of government surveillance. In the 2012 case *United States v. Jones*, the Court found that warrantless GPS tracking of an individual's movements for an extended period of time contravened the parameters set in *Smith*.[101] The two concurrences in *Jones* further suggested reworkings of the *Smith* framework in light of changing technology and an increased need for robust privacy protection given the government's ability to access telephonic data with ease.[102] The opinion in *Klayman* focused on *Jones* to illustrate the need to rethink the nature and scope of privacy given the vastly different use of technology of today as compared to the 1970s, when *Smith* was decided.[103] In mid-2014, the Supreme Court followed this rights-protective line of reasoning when it decided *Riley v. California*, holding that warrantless searches of the electronic contents of an arrestee's cell phone were in

---

[98] *Id.* at 61.

[99] As of this writing, *Klayman* and *Clapper II* are under appeal before the D.C. Circuit Court of Appeals and the Second Circuit Court of Appeals, respectively. Both cases have been briefed and oral arguments were heard in Fall 2014.

[100] *See e.g.*, Matthew Barakat, *Scalia Expects NSA Program to End Up in Court*, ASSOCIATED PRESS (Sept. 25, 2013), *available at* http://news.yahoo.com/scalia-expects-nsa-wiretaps-end-court-145501284—politics.html. In a speech to the Northern Virginia Technology Council, Justice Scalia stated:

> [W]hether the NSA can do the stuff it's been doing . . . which used to be a question for the people . . . will now be resolved by the branch of government that knows the least about the issues in question, the branch that knows the least about the extent of the threat against which the wiretapping is directed.

Id.

[101] United States v. Jones, 132 S. Ct. 945, 954 (2012).

[102] *See id.* at 954 (Sotomayor, J., concurring). Justice Sotomayor argued that warrantless surveillance that involves no physical trespass but mines and stores a large volume of data may still be subject to classification as a "search" for Fourth Amendment purposes. *Id.* She noted that such surveillance, especially in today's society, has the potential to "chill[] associational and expressive freedoms," and "is susceptible to [government] abuse." *Id.* at 956; *see also id.* at 957 (Alito, J., concurring). Justice Alito would evaluate Fourth Amendment claims based on the reasonable expectation of privacy of individuals, taking into account the changing nature of this expectation as technology advances. *Id.* at 958. Justice Alito notes that legislation that curtails warrantless surveillance may be the best action to deal with the questions left open by *Jones,* but notes that such legislation does not seem to have materialized at the state or federal level. *Id.* at 964.

[103] Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013).

violation of the Fourth Amendment protections against unreasonable search and seizure.[104]

These rights-protective perspectives—offered by justices with different political and theoretical perspectives—may offer a preview of a significant jurisprudential shift not only in hearing security-related cases on their merits, but in finding for plaintiffs alleging privacy and civil liberties infringements. However, the historically deferential attitude of courts toward matters of national security, a stance that has only compounded in the post-9/11 context, suggests that this may continue to be an uphill battle for civil libertarians.[105]

More troubling to proponents of the efficacy of existing legislative and executive accountability mechanisms are the disclosures made by Snowden. These mechanisms were revealed to be either theoretical or passive until significant leaks forced a public discourse that demanded a more active accountability regime. In fact, the federal government exploited the lack of transparency and effective accountability mechanisms until the start of the Snowden disclosures to secure dismissals like that in *Clapper I* and to circumvent efforts of criminal defendants to discover whether they had been actually surveilled.[106]

Reliance on sporadic leaks to trigger genuine accountability is structurally problematic.[107] Our reliance on leaks thus far should force us to reconsider the extreme secrecy under which intelligence-gathering programs, like the NSA Metadata Program, are administered, and to consider means by which institutional actors can exert meaningful and regular oversight and control over these programs. Such change would force politicians to take ownership over secret counterterrorism programs, weighing their expediency against possible constitutional defects or the judgment of public opinion. An atmosphere in which accountability mechanisms are not merely ersatz pending an illegal leak could provide space for genuine public discourse and at least the possibility of greater protection of civil liberties.

III. COMPARATIVE PERSPECTIVES ON SURVEILLANCE AND ACCOUNTABILITY

Both the United Kingdom and India have struggled greatly with establishing effective surveillance mechanisms and with maintaining privacy rights and civil liberties. As democracies with a shared legal background and ongoing intelligence sharing, yet with different government and accountability structures, these nations provide useful comparisons to the United States in terms of examining the efficacy of counterterrorism surveillance and the concomitant strength of accountability measures and safeguards.

---

[104] Riley v. California, 134 S.Ct. 2473 (2014).

[105] *See generally* Setty, *supra* note 86.

[106] *See, e.g.*, David Kravets, *Feds Won't Say If NSA Surveilled New York Terror Suspects*, WIRED (May 13, 2013), http://www.wired.com/2013/05/feds-mum-on-terror-suspects/.

[107] *Cf.* RAHUL SAGAR, SECRETS AND LEAKS: THE DILEMMA OF STATE SECRECY (Princeton Univ. Press 2013) (arguing that the status quo of incomplete oversight coupled with sporadic leaks is the best realistic option for national security accountability); David Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512 (2013) (describing ways in which leaks are an integral and adaptive mechanism of information disclosure for the US federal government).

A. United Kingdom

The United Kingdom has been dealing with internal and external security threats for decades. Shortly after the end of World War II, the United Kingdom recognized the dual needs of access to global intelligence and protection of its own privacy interests from the intelligence-gathering operations of enemies and allies alike. Thus, in the early Cold War era, the United Kingdom and United States entered into what is now known as the UKUSA Agreement, which structured intelligence sharing and prohibited spying on each other.[108] This relationship has grown over the decades, and remains a strong one. However, U.K. legislative and judicial responses to terrorism and security-related threats have evolved in a somewhat different direction, reflecting domestic statutes and court decisions that are responsive to both internal politics and pressures as well as European Union-level mandates on counterterrorism activities and constraints on intrusions into the private lives of individuals living within the European Union.[109]

Although the NSA Metadata Program has garnered significant global publicity and criticism, telecommunications providers within the European Union have been collecting and retaining E.U. telephonic and Internet metadata for extended periods of time since at least 2006. This collection has been a topic of much discussion and has spawned multiple directives within the United Kingdom and by the European Union. This practice and has recently been discontinued. Tracing how the United Kingdom's domestic counterterrorism agenda, including bulk metadata collection, has developed in conjunction with and in response to EU-level directives, sheds light on an alternative approach to balancing security needs and accountability on these matters.

The United Kingdom's Regulation of Investigative Powers Act ("RIPA"), implemented in 2000, authorized a significant amount of domestic and external data collection, but also instituted some safeguards to protect privacy interests.[110] Among these was the creation of the Investigative Powers Tribunal, which was granted jurisdiction over individual complaints related to the conduct of intelligence services.[111] In 2002, the European Union adopted a Directive on Privacy and Electronic Communications[112] that, among other things, ensured that the privacy of individuals using telephones and the internet to communicate was maintained even in light of rapidly evolving technology, and mandated the destruction of data held by telecommunications companies and internet providers after billing and other such purposes had been fulfilled.[113]

---

[108] *See* Amendment No. 4 to the Appendices to the UKUSA Agreement, May 10, 1955, *available at* http://www.nsa.gov/public_info/_files/ukusa/new_ukusa_agree_10may55.pdf (reaffirming the terms of the original March 1946 agreement and expanding the treaty to include Canada, Australia, and New Zealand, thus creating the Cold War intelligence arrangement sometimes referred to as the "Five Eyes."). *See generally* Paul Farrell, *History of 5-Eyes—Explainer*, GUARDIAN (Dec. 2, 2013), *available at* http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer.

[109] For a thorough discussion of the multi-layered system of protecting fundamental rights in the European Union, see FEDERICO FABBRINI, FUNDAMENTAL RIGHTS IN EUROPE: CHALLENGES AND TRANSFORMATIONS IN COMPARATIVE PERSPECTIVE (2014).

[110] Regulation of Investigatory Powers Act, 2000, c. 23, (U.K.) [hereinafter RIPA].

[111] RIPA, *supra* note 110, § 65.

[112] Eur. Parl. Directive 2002/58/EC, *On Privacy and Electronic Communications*, July 12, 2002.

[113] *Id.* ¶¶ 7, 20, 22.

In 2006, partially in reaction to the 2004 Madrid train bombing and the 2005 London underground bombings, the European Union adopted Directive 2006/24/EC. [114] The directive amended previous directives and mandated, in accordance with the principle of proportionality and with respect for individual privacy, that domestic telephonic and internet metadata be retained by telecommunications companies for law enforcement and counterterrorism investigatory purposes for six to twenty-four months.[115]

Because of the systematic data retention mandated by Directive 2006/24/EC and the extensive and intrusive surveillance technology known to be used by the government,[116] numerous parliamentary committees have undertaken investigations of the surveillance apparatus in the United Kingdom. A broad investigation by the Constitution Committee led to findings in 2009 that the intelligence-gathering services were largely compliant with the law, but that report included numerous recommendations for changes to surveillance authority and transparency. Among the recommendations were giving greater consideration to civil liberties before implementing further surveillance programs,[117] granting greater authority to various commissioners to exercise increased oversight,[118] revisiting existing legislation to increase specificity in the surveillance authority,[119] and making the work and role of the Investigatory Powers Tribunal more visible to the public.[120] Since the tribunal operates and deliberates in secret, offers limited procedural and substantive rights, and has never ruled in favor of a complainant, the tribunal is open to critique that, like the FISC in the United States, it merely rubber stamps decisions made by the intelligence agencies and masks a lack of genuine accountability for government abuse of civil liberties.[121] Increased transparency over the tribunal's operations may help boost its efficacy as a constraining institution on the U.K. intelligence community and, in fact, has already given the public better insight into the operations of the tribunal and the types of issues it is

---

[114] Eur. Parl. Directive 2006/24/EC, *On the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC*, March 15, 2006, ¶ 10 (acknowledging the need for revised intelligence-gathering procedures in light of recent terrorist acts).

[115] *Id.*, art. 5 (describing categories of metadata to be retained); *id.* art. 6 (mandating retention for at least six months and not more than two years). It is noteworthy that the United Kingdom, along with 15 other members of the European Union, declared its intention to postpone application of the directive to internet data; Declaration by the United Kingdom pursuant to Article 15(3) of Directive 2006/24/EC.

[116] *See* Clive Walker, *Championing Local Surveillance in Counter-Terrorism*, *in* Fergal Davis, et al., SURVEILLANCE, COUNTER-TERRORISM AND COMPARATIVE CONSTITUTIONALISM 24 (2014) (describing the U.K. government's "all-risks surveillance" approach to detecting terrorism threats before they are actualized).

[117] Constitution Committee, *Second Report, Surveillance: Citizens and the State*, 2008-9, H.L.18-I, ¶¶ 110, 144; *see also id.* ¶ 307 (recommending that the government amend the Data Protection Act 1998 to require the issuance of an independent, public, and detailed Privacy Impact Assessment prior to the adoption of any new surveillance or information collection).

[118] *Id.* ¶¶ 137, 231, 237, 436.

[119] *Id.* ¶¶ 357, 379.

[120] *Id.* ¶ 259.

[121] *See, e.g.*, Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1171–72 (2006) (arguing that the Investigatory Powers Tribunal, charged with reviewing complaints as to surveillance impermissibly infringing on civil rights, lacked operational transparency and functionally added nothing to existing mechanisms to protect individual rights).

hearing.[122] However, because the tribunal only acts when a complaint is brought to it, even if it were functioning in a fair and impartial manner, it is structurally unable to act as a comprehensive check on government abuse.[123]

As in the United States, the Snowden disclosures that began in June 2013 prompted additional reviews of the various programs in which British intelligence agencies were involved, including those that related to telephonic and Internet data collection and retention. Among the Snowden disclosures were: the extent to which the United Kingdom's signals intelligence organization, Government Communications Headquarters ("GCHQ"), worked with the NSA on counterencryption efforts used in the United States, United Kingdom, and elsewhere;[124] the progress of GCHQ's own counterencryption effort;[125] GCHQ's receipt of data from the NSA's PRISM program to intercept and store data from internet service providers;[126] and GCHQ's interception and storage of images from webcam chats.[127]

An investigation by the Intelligence and Security Committee of the Parliament considered the question[128] of whether GCHQ's receipt of information from the NSA via the PRISM program was legal, conducting its analysis under the statutory framework of the Intelligence Services Act,[129] Regulation of Investigatory Powers Act,[130] and the Human Rights Act.[131] The committee ultimately found that

---

[122] *See* Katrin Bennhold, *In Britain, Guidelines for Spying on Lawyers and Clients*, N.Y. TIMES (Nov. 6, 2014), *available at* http://www.nytimes.com/2014/11/07/world/europe/in-britain-guidelines-for-spying-on-lawyers-and-clients.html (discussing the Investigatory Powers Tribunal's order to disclose government documents related to the practice of intercepting communications between clients and their attorneys); *see also Government Forced to Release Secret Policy on Surveillance of Lawyers*, REPRIEVE (Nov. 6, 2014), http://www.reprieve.org.uk/press/2014_11_06_uk_govt_force_release_spying_lawyers/

[123] *See* Walker, *supra* note 116, at 32.

[124] *See* Nicole Perlroth, Jeff Larson, & Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES (Sept. 6, 2013), *available at* http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all (discussing coordination between the NSA and GCHQ on the Bullrun program, an effort to penetrate encryption barriers on online communications).

[125] *See id; see also* James Ball, Julian Borger, & Glenn Greenwald, *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, GUARDIAN (Sept. 5, 2013), http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (describing the Edgehill program).

[126] *See GCHQ Use of Prism Surveillance Data was Legal, Says Report*, BBC (July 17, 2013), http://www.bbc.com/news/uk-23341597.

[127] *See* Spencer Ackerman & James Ball, *Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ*, GUARDIAN (Feb. 27, 2014), http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo (describing a GCHQ initiative supported by the NSA that captured images from Yahoo! account users' webcam chats from 2008 to 2012).

[128] *See* Statement from the Intelligence and Security Committee of Parliament on GCHQ's Alleged Interception of Communications under the US PRISM Programme (July 17, 2013), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225459/ISC-Statement-on-GCHQ.pdf.

[129] Intelligence Services Act, 1994, c. 13 (U.K.). This act authorizes the activity of secret intelligence surveillance for national security purposes and requires minimization procedures to limit the impact of surveillance on privacy rights. *See id.* §§ 1–3.

[130] *See* RIPA, *supra* note 110, §1(1) (authorizing the interception of communications for certain purposes). RIPA further authorizes the interception of external communications if warranted by the Secretary of State, as was the case with regard to the Prism program. *See id.* §§ 8(4)–(5).

[131] Human Rights Act, 1998, c. 42 (U.K.). The aim of this Act is to give domestic effect to the rights contained in the European Convention on Human Rights.

GCHQ's actions with regard to PRISM were compliant with the statutory framework, but concluded that the parameters of surveillance authority required additional specificity and consideration.[132] That reconsideration of potential reforms to curtail authority was taken up by a variety of legislators but did not gain significant purchase in Parliament.

Further frustrating the cause of civil libertarians is the fact that, under RIPA, the sole recourse for challenging such actions under U.K. law is making a claim to the Investigatory Powers Tribunal. While the Human Rights Act 1998 incorporates the European Convention on Human Rights ("ECHR") into U.K. domestic law, thus permitting the judiciary to declare incompatibility if it believes that a national security measure is incompatible with the ECHR standard, this does not constitute a mandate that the domestic security apparatus change its policies.[133] As such, review at the domestic level has often been sharply curtailed, and review at the supranational level potentially offers a more fruitful avenue to pursue civil liberties claims.

Although the Treaty of the European Union provides that "national security remains the sole responsibility of each Member State,"[134] the question of how to resolve conflicts between domestic security measures and the robust privacy and dignity protections under various European Union conventions and treaties is complicated and to some extent remains unresolved. The European Convention on Human Rights provides a number of protections for individuals, including the right to respect for an individual's private and family life, his home, and his correspondence.[135] However, that provision is followed by a caveat that allows for wide latitude for government intrusions on privacy when they are "in accordance with the law and [are] 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."[136] This national security exception is broadly enough drafted such that it may, in many instances, swallow the privacy right altogether.[137]

For residents of the United Kingdom, a similar dynamic exists with regard to the European Union Charter of Fundamental Rights: The text of the charter contains a broad and thick privacy protection for personal life and data,[138] but the United Kingdom has acceded to the charter and to the 2009 Treaty of Lisbon with the reservation of opt-outs that—at least arguably—allow U.K. authorities to escape

---

[132] *See* Statement from the Intelligence and Security Committee of Parliament on GCHQ's Alleged Interception of Communications under the US PRISM Programme, *supra* note 128, ¶ 7.

[133] Human Rights Act, 1998, c. 42 (U.K.) § 4.

[134] Consolidated Version of the Treaty on European Union and the Treaty on the Functioning of the European Union art. 4, Oct. 26, 2012, 2012 O.J. (C 326) 18.

[135] Convention for the Protection of Human Rights and Fundamental Freedoms art. 8(1), Nov. 4, 1950, E.T.S. No. 5 [hereinafter ECHR].

[136] *Id.* art. 8(2).

[137] This is particularly true in cases in which a government could invoke Article 15 of the ECHR, allowing a country to derogate from its obligations in times of national emergency. *E.g.*, A. v. United Kingdom, 2009-II Eur. Ct. H.R. 137, ¶¶ 181, 190 (finding that the derogation must be in response to imminent national emergency and the scope of the derogation can be evaluated for proportionality).

[138] *See* Charter of Fundamental Rights of the European Union, arts. 7, 8, Dec. 18, 2000, 2000 O.J. (C 364) 1 (discussing protection of private and family life, as well as personal data, respectively).

broad privacy protections in matters that touch on the areas of freedom, security, and justice.[139] Likewise, the previously discussed 2002 E.U. directive lays out the importance of protecting privacy and confidentially of electronic communications,[140] but also allows member states to create policies that undercut those protections if necessary to safeguard national security and public safety, among other exceptions.[141] Following this pattern of allowing broad privacy protections to be compromised for national security purposes, case law before the European Court of Human Rights has made clear that privacy rights can be curtailed for the sake of counterterrorism efforts.[142]

In this patchwork of protections and compromises, various bodies within the European Union are attempting to react to the Snowden disclosures. Soon after the disclosures regarding the scope and invasiveness of GCHQ intelligence-gathering, the European Parliament began to step up its consideration of how much primacy to give privacy concerns, and U.K. plaintiffs[143] began the process of seeking relief from surveillance and the collection of metadata from the European Court of Human Rights.[144] A suit currently pending queries whether Article 8 of the ECHR has been abrogated by the actions of GCHQ.[145]

Complementing this suit is the April 2014 opinion in the *Digital Rights*[146] case by the European Court of Justice weighing the question of the retention and use of telecommunications metadata by intelligence agencies. The ECJ declared the 2006 Data Retention Directive invalid based on its concern that "by requiring the retention of [extensive] data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data."[147] In language echoing the concerns of Judge Leon in the U.S. *Klayman*

---

[139] The United Kingdom's opt-out in these areas attempts to preserve the national autonomy that existed before 1999, in the pre-Treaty of Amsterdam era, in which various "pillars" of the European Union, including matters of security and justice, were reserved in large part for national policymakers. *See* Consolidated Version of the Treaty on European Union and the Treaty on the Functioning of the European Union, Protocol 21, Sept. 5, 2008, 2008 O.J. (C 115) 295 (governing U.K. participation in EU matters pertaining to Justice and Home Affairs). Under Protocol 21, the United Kingdom has the right to opt-in on various EU legislation and the implementation of European Court of Justice decisions. *Id.* There is ongoing disagreement as to the scope of the protections of the Treaty of Lisbon and the carve-out in Protocol 21 for U.K. citizens.

[140] *See generally* Directive 2002/58 of the European Parliament and of the Council of 31 July 2002 on Privacy and Electronic Communications, 2002 O.J. (L 201) 37.

[141] *Id.* art. 15(1).

[142] Klass v. Germany, App. No 5029/71, 28 Eur. Ct. H.R. (ser. A), ¶ 48 (1978).

[143] Article 13 of the ECHR guarantees an effective remedy for anyone within an EC nation whose rights have been violated.

[144] *See* Steven Erlanger, *Britain: Online Surveillance Challenged*, N.Y. TIMES (Oct. 3, 2013), http://www.nytimes.com/2013/10/04/world/europe/britain-online-surveillance-challenged.html?_r=0.

[145] Big Brother Watch v. United Kingdom, App. No 58170/13, Eur. Ct. H.R. (2013), *communicated* Jan. 9, 2014.

[146] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd. v. Minister for Communication and *Kärtner Landesregierung*, 2014 O.J. (C 175) 6.

[147] Press Release, Court of Justice of the European Union, The Court of Justice declares the Data Retention Directive to be Invalid, (Apr. 8, 2014) (on file with the *Stanford Journal of International Law*). The ECJ noted that the type of metadata collected under Directive 2006/24/EC would allow for someone to know the identity of everyone with whom a particular subscriber communicates, the time and place of communication, and the frequency of communications between a subscriber and his/her contacts. This comprehensive information that can be gleaned from this mass, non-individualized metadata collection prompted the ECJ to find that too much precise information on the private lives of

decision, the ECJ made clear that the protection of privacy rights needed to increase along with the online presence of most individuals and the concomitant power of the government to surveil them.[148]

The suit pending at the European Court of Human Rights and the ECJ decision in the *Digital Rights* case offer a strong indication that supranational review on the surveillance regimes of member nations may yield significant protections for individual privacy rights. In some ways, these cases follow on ECJ decisions over the last several years that affirm human rights even when conflicting national security policies are asserted as necessary by the national governments of member states.[149] Yet the decision in *Digital Rights* may not necessarily translate into nullification of metadata collection and retention in individual nations, such as the United Kingdom, particularly given the leeway that individual member states have in implementing protections under the European Convention on Human Rights, as well as the likelihood of the intelligence community to exploit ambiguities in the patchwork of domestic and E.U. law and regulations.[150]

Further, we are still left with the question of whether these direct accountability mechanisms, the Investigatory Powers Tribunal on the domestic level or the availability of bringing suit before the European Court of Human Rights, actually provide meaningful accountability and constraint on government surveillance without the existence of leaked information like that supplied by Snowden in 2013. These reactive mechanisms would not have been triggered without leaked information; combined with a permissive legislative framework for surveillance and the secrecy surrounding surveillance activities in the United Kingdom, those interested in learning more about the scope and depth of surveillance activities and challenging those activities may still need to rely on leaked information to trigger mechanisms that could help promote the rule of law.

B. India

The authority of Indian intelligence agencies to conduct warrantless surveillance and data collection is long-standing and broad, and does not include effective checks—judicial or otherwise—to control against potential abuse. Authority for current policies of warrantless wiretapping and surveillance, like many of India's counterterrorism authorities, finds its roots in colonial-era legislation that was meant to control the Indian population and prevent possible

---

subscribers was being made available in a way that impermissibly interfered with the right to respect for private life and the protection of personal data. *Id.*

[148] Scholars have described the *Digital Rights* decision as a milestone in its efforts to entrench, strengthen and constitutionalize EU-level privacy protection. *See* Federico Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.*, 28 HARV. HUMAN RTS. J. (forthcoming 2015).

[149] *See* Joined Cases C-402/05 P & C-415/05 P, Kadi, Al Barakaat v. Council of the European Union, 2008 E.C.R. I-6351 (voiding the terrorist designation of an individual without due process); *see also* Joined Cases C-584/10 P, C-593/10 P, & C-595/10 P, Council, Comm'n and United Kingdom v. Kadi, ECLI:EU:C:2013:518 (E.C.R. Jul. 18, 2013) (finding that the process provided prior to the designation of an individual as a terrorist was insufficient to comport with EU human rights standards).

[150] *See* Governing Intelligence Symposium, Stanford Law School, May 2, 2014 (this portion of the symposium was held under Chatham House rules) (notes on file with author).

uprisings against the British colonial government.[151] The Indian Telegraph Act of 1885 specifically authorizes the interception and storage of telegraph messages by the central or state governments in times of "public emergency, or in the interest of the public safety" if it is deemed necessary or expedient to do so "in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence."[152] This permissive language set the stage for over a century of legislation, executive action, and judicial permission that enabled broad surveillance of all forms of telecommunications, even in peace time, so long as such surveillance has a security-related nexus.

The Indian government has continued to focus on national security threats since its independence in 1947; as such, India's legal security framework includes constitutional, executive, and statutory emergency powers.[153] Indian authorities also depend on non-emergency criminal ordinances and laws that authorize broad police powers that in many ways mirror emergency and counterterrorism-related powers. This conflation of various legal bases for authority—constitutional emergency powers, counterterrorism law, and criminal law—into one system has led to an extraordinary amount of power being granted to intelligence and counterterrorism authorities[154] as long as they have articulated that their actions are being taken for the benefit of national security.[155]

Broad counterterrorism powers, including surveillance authority, have incrementally increased over time.[156] In the last fifteen years, this dynamic can be traced both to perceived domestic intelligence failures and the shifts in the international community in response to the September 11, 2001 attacks in the United States. The Kargil Conflict of 1999, precipitated by the Pakistani military crossing the Line of Control[157] and involving several months of warfare between Pakistan and India before the restoration of the Line of Control, prompted

---

[151] *See generally* Anil Kalhan et al., *Colonial Continuities: Human Rights, Terrorism, and Security Laws in India*, 20 COLUM. J. ASIAN L. 93 (2006) (examining India's current security and antiterrorism laws from an historic and institutional perspective).

[152] *See* The Indian Telegraph Act, No. 13 of 1885, INDIA CODE (1993), § 5, *available at* http://indiacode.nic.in.

[153] *See* INDIA CONST. arts. 352–56, *amended by* Constitution (Ninety-fourth Amendment) Act, 2006 (emergency powers provisions); *see also* GRANVILLE AUSTIN, WORKING A DEMOCRATIC CONSTITUTION: A HISTORY OF THE INDIAN EXPERIENCE 295–97 (2003) (discussing the era of Emergency Rule).

[154] *See* Sudha Setty, *What's in a Name? How Nations Define Terrorism Ten Years After 9/11*, 33 U. PA. J. INT'L L. 1, 48–54 (2011) (describing the circumscribed rights of defendants in terrorism investigations and prosecutions).

[155] *See* People's Union for Civil Liberties v. Union of India, A.I.R. (1997) S.C. 568, ¶¶ 5–6 (India) (holding that the Indian Telegraph Act of 1885 authorized broad surveillance only when authorities were undertaking such surveillance under the circumstances of emergency or heightened security threat). The Supreme Court directed the government to improve procedural safeguards to protect against potential abuse of these authorities. *Id.* ¶¶ 34–35.

[156] *See* Ujjwal Kumar Singh, *Surveillance Regimes in Contemporary India*, in Davis, *supra* note 116, at 42–44. Singh cites the government's use of The Terrorist and Disruptive Activities (Prevention) Act, 1985, No. 31, Acts of Parliament, 1985 (India); The Prevention of Terrorism Act, 2002, No. 15, Acts of Parliament, 2002 (India); and the Unlawful Activities (Prevention) Amendment Act, 2008, No. 35, Acts of Parliament, 2008 (India) as statutes that promote a "notion of danger that could no longer be contained by ordinary policing." *Id.* at 43.

[157] The Line of Control represents the geographic boundaries of political and military control between India and Pakistan in the contested Kashmir region.

investigation as to how the Indian intelligence community could use surveillance technology to act preventatively against potential military and/or terrorism threats.[158] The post-conflict analysis by the Kargil Review Committee noted the need for the Indian government to not undervalue intelligence analysis to prevent even an unlikely attack.[159]

The lack of ability to analyze relevant information and to share that information among intelligence agencies, the military, and law enforcement were seen as serious obstacles that needed to be resolved,[160] and the Indian government looked to increase its technological intelligence-gathering capabilities to improve the chances of forestalling another Kargil-type conflict.[161] However, the Kargil Review Committee observed that the cost in human and material resources required to "plug all conceivable loopholes to frustrate every eventuality, howsoever foolhardy . . . would have been neither militarily nor politically cost-effective."[162] The Committee went further to note that if the government were to adopt a zero-tolerance stance toward such attacks, this would have invited legitimate criticism as to resource allocation and would have weakened the ability of India to defend itself effectively against Pakistan.[163] In the end, the post-Kargil analysis did not emphasize a need for greater legal authority for surveillance. Instead, the focus was on technological expertise and better information sharing within the government.

Yet two years after the Kargil Conflict, the events of September 11, 2001, and the subsequent international pressure to strengthen domestic counterterrorism efforts, including surveillance, intelligence-gathering, and intelligence-sharing, led to significant statutory reform in India.[164] The Parliament of India passed the Prevention of Terrorism Act, 2002 (POTA) partially in response to the United Nations Security Council's Resolution 1373 and its global mandate to fight terrorism.[165] POTA laid out specific procedures for requesting the interception of telecommunications of terrorism suspects that required some reasonable suspicion

---

[158] *See* India Kargil Review Committee, *From Surprise to Reckoning: The Kargil Review Committee Report, Executive Summary*, http://nuclearweaponarchive.org/India/KargilRCA.html (visited Feb. 19, 2014) (noting that the surprise nature of the Kargil attack highlighted the failure of intelligence agencies to gather the relevant information and to share it with law enforcement and military. The summary concluded that "[t]here is need for greater appreciation of the role of intelligence and who needs it most and also more understanding with regard to who must pursue any given lead. It further highlights the need for closer coordination among the intelligence agencies.").

[159] The Kargil Review Committee's report notes that the Pakistani military's position in Kargil was, over the long term, untenable: "[The attack] was at best a political gamble, but otherwise so irrational and implausible as to have been virtually ruled out by the India side which was in any case exclusively focused on infiltration, not on intrusion or invasion. The lesson, if any, is that an irrational or rogue action can never be ruled out." GOV. OF INDIA, FROM SURPRISE TO RECKONING: THE KARGIL REVIEW COMMITTEE REPORT 22 (Sage Publishing 2000) [hereinafter Kargil Committee Report].

[160] *See* ASHLEY J. TELLIS, C. CHRISTINE FAIR & JAMISON JO MEDBY, LIMITED CONFLICTS UNDER THE NUCLEAR UMBRELLA: INDIAN AND PAKISTANI LESSONS FROM THE KARGIL CRISIS 20 (2001) (highlighting the discontent among government actors and the public with the performance of Indian intelligence agencies).

[161] TELLIS, *supra* note 160, at 70–72.

[162] Kargil Committee Report, *supra* note 159, at 220.

[163] *See id.*

[164] *See* Setty, *supra* note 154, at 51–52.

[165] See V. Venkatesan, *The POTA Passage*, 19 FRONTLINE, Apr. 13, 2002, at 13 (noting that various cabinet ministers had encouraged the passage of POTA in parliamentary debates based on the mandate of Resolution 1373).

on the part of investigators.[166] When POTA was repealed in 2004 as part of a political pledge to deal with human rights abuses, intelligence agencies could still rely on the broad surveillance powers authorized by the Indian Telegraph Act of 1885 to collect and analyze telephony and electronic data as related to security matters.

The government expanded these powers after the November 2008 terrorist attacks in Mumbai,[167] when it quickly passed counterterrorism legislation that broadened and made permanent the powers previously granted under POTA, as well as amended the Information Technology Act 2000. These amendments allowed for surveillance of all digital communications of all individuals within India, regardless of whether security threats were at issue.[168] The amendments also made clear that the scope of warrantless surveillance authority includes all types of telephony data and internet data, as distinguished from the metadata collection authorized by the United States and United Kingdom.[169]

By 2009, the government had leveraged the authority granted in 1885 and 2008 to announce creation of the Central Monitoring System (CMS), a data collection and analysis system meant to capture all electronic data throughout India.[170] The parameters of this program are secret and, despite efforts to create privacy legislation that could work to curtail the reach of the CMS and to challenge the constitutionality of the CMS in court, it continues to operate without external oversight.[171]

Given the deference of the Indian judiciary with regard to national security initiatives and the ongoing attacks that have buoyed public support for extremely strong counterterrorism powers, it is unclear whether the Indian judiciary would find a constitutional violation in the type of surveillance authorized under the 2008 amendment to the Information Technology Act, or that which is perhaps taking place under the CMS. On one hand, the Supreme Court has previously interpreted Article 21 of the Indian Constitution, which articulates the fundamental right to life, as including privacy of persons and personal thought.[172] The Court has used its interpretation of Article 21 as the basis for inferring the need for procedural

---

[166] *See* Prevention of Terrorism Act, 2002, No. 15, Acts of Parliament, 2002 (India).

[167] *See* Somini Sengupta & Keith Bradsher, *India Faces a Reckoning as Terror Toll Eclipses 170*, N.Y. TIMES, Nov. 30, 2008, at A1 (questioning whether Indian authorities could have prevented the attack with better intelligence analysis).

[168] *See* Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India) (authorizing broad data collection and analysis regardless of whether such investigation is related to an emergency or national security matter).

[169] *Id.*

[170] *See* Rajya Sabha, Ministry of Commc'ns & Info. Tech, *Centralised System to Monitor Communications*, PRESS INFO. BUREAU (Nov. 26, 2009, 17:50 IST), http://pib.nic.in/newsite/erelease.aspx?relid=54679 (noting that the system was necessary "to strengthen the security environment in the country").

[171] *See* HUMAN RIGHTS WATCH, *India: New Monitoring System Threatens Rights* (June 7, 2013), http://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights (detailing the need for greater transparency over the operation of the CMS and proposed privacy legislation to curb the reach of the CMS); *see also* Pranesh Prakash, *Can India Trust Its Government on Privacy?*, N.Y. TIMES (July 11, 2013), http://india.blogs.nytimes.com/2013/07/11/can-india-trust-its-government-on-privacy/?_php=true&_type=blogs&_r=0.

[172] *See* Kharak Singh v. State of Uttar Pradesh, (1964) 1 S.C.R. 332 (India) (holding that the meaning of personal liberty as guaranteed under Article 21 of the Indian Constitution included a citizen's freedom from encroachments on private life).

safeguards against potentially abusive and overly intrusive surveillance.[173] However, the Indian judiciary has historically been extremely deferential to legislative and executive decision-making on counterterrorism matters, even when human rights and civil liberties are at stake,[174] making the courts a largely unreliable source of rights-protective constraints.[175]

IV. INCREASING REAL ACCOUNTABILITY

The comparative analysis in the previous sections of this paper reveals some common themes: ever increasing technological capabilities of the intelligence community; sustained pressure to use that technology to prevent terrorist plots from developing; broad, conflicting, and sometimes unclear legal authorities to conduct massive surveillance and data collection; the intelligence community leveraging lack of transparency to maximize its surveillance; and the question of whether existing accountability measures in the United States, the United Kingdom, and India are sufficient to maintain the rule of law and protect individual rights.

Although many of the challenges in these nations are the same, the paths toward genuine accountability differ based on the current level of transparency, the types and strength of review mechanisms available, and the public support for mass data collection and surveillance. In India, there appears to have been a modest degree of transparency regarding mass data collection: The Indian public, politicians, and the judiciary have long understood that the Indian Telegraph Act of 1885 authorizes such collection when the government can articulate a security nexus. Further, unlike the somewhat vague language of Section 215 of the Patriot Act, the power granted under the Information Technology (Amendment) Act of 2008 is clear in its scope, and the Indian government itself announced the roll-out of the CMS.

However, the precise scope of actual data collection and surveillance remains murky, especially as the intelligence community's capabilities have increased with programs such as the CMS. It is yet to be seen whether objections to the intrusiveness of the CMS will resonate with Indian politicians such that comprehensive privacy legislation is enacted and parliamentary oversight of surveillance programs is strengthened, or with the Indian judiciary such that the previous articulation of the right to privacy under Article 21 of the Indian Constitution will protect against the type of massive data collection capable under a fully operational CMS. In some respects, this depends on the views of the Indian public and the willingness of the judiciary to engage in security matters in a way that would break with its highly deferential past.

In the United Kingdom, a different set of avenues for accountability exists. The opinion in the European Court of Justice *Digital Rights* case includes strong language on the need to dismantle systemic metadata collection and storage in order

---

[173] People's Union for Civil Liberties v. Union of India, A.I.R. (1997) 1 S.C.C. 568 (India).

[174] *See generally* Mrinal Satish & Aparna Chandra, *Of Maternal State and Minimalist Judiciary: The Indian Supreme Court's Approach to Terror-Related Adjudication*, 21 NAT'L LAW SCH. OF INDIA REV. 51 (2009) (assessing the Indian Supreme Court's lack of effectiveness in providing a judicial check on overreaching counterterrorism policies).

[175] *See* Surabhi Chopra, *National Security Laws in India: The Unraveling of Constitutional Constraints*, 16 OR. REV. INT'L L. at 61–64, 73–78 (2014).

to preserve fundamental privacy and dignity rights of individuals. This shift, along with other recent movement on privacy rights, suggests institutions at the European level are at the forefront of protecting privacy over electronic data. However, the lack of transparency as to what programs are actually in place presents a knotty problem: If the United Kingdom continues domestic metadata collection practices in secret based on its interpretation that security-related policy cannot be dictated at the European level, is there any accountability measure in place that could forestall it? The domestic Investigative Powers Tribunal would not review mass collection if it were not brought to the attention of a complaining party. Likewise, European-level judicial review would depend on a public understanding of the scope and type of surveillance at issue. Without a Snowden-like disclosure to enable such review or a strong commitment by the United Kingdom to abide by the human rights standards articulated at the European level, parliamentary oversight would be the key mechanism to protect against overreaching by the British intelligence community, akin to the legislative oversight structure in India.

Although Congress could launch a large-scale investigation into the programs Snowden disclosed, like the Church Committee in its time,[176] its ability to serve effectively as an ongoing accountability mechanism over intelligence gathering in the manner of a parliament seems unlikely. For the political and structural reasons discussed above, the apparatus of national security policy-making is somewhat intentionally insulated from Congress. On the one hand, the benefit of this structural arrangement is that it may facilitate expertise and efficient decision-making, but a key effect is also that this apparatus is not really accessible to the other branches of government or the public.[177] This consolidation of decision-making authority in the executive branch, plus the difference between congressional and parliamentary access to executive branch information, accounts for a different potential for legislative oversight in the United States as compared to the United Kingdom and India. Further, the lack of widespread and sustained public pressure

---

[176] *See* Frederick A.O. Schwarz, Jr., *Why We Need a New Church Committee to Fix Our Broken Intelligence System*, BRENNAN CTR. FOR JUSTICE (Mar. 12, 2014), http://www.brennancenter.org/analysis/why-we-need-new-church-committee-fix-our-broken-intelligence-system. Schwarz, who served as chief counsel to the Church Committee, argues that the type of deep, wide-access investigation that the Church Committee undertook served the purposes of uncovering illegal government behavior, increasing self-policing and the inculcation of best practices among government agencies, and restoring public confidence in the government as being bound by laws. *Id.* Senator Frank Church, chair of the Church Committee, recognized the inability to maintain accountability over NSA activities from within the administration:

> "[The NSA's] capability at any time could be turned around on the American people, and no American would have any privacy left, such [is] the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide . . . . I know the capacity that is there to make tyranny total in America, and we must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is the abyss from which there is no return."

See James Bamford, *The Agency That Could Be Big Brother*, N.Y. TIMES (Dec. 25, 2005), http://www.nytimes.com/2005/12/25/weekinreview/25bamford.html?pagewanted=all&_r=1& (quoting Senator Frank Church from statements made in 1975).

[177] *See generally* Aziz Rana, *Who Decides on Security?*, 44 CONN. L. REV. 1417 (2012) (arguing that the process of national security decision making has been narrowed inappropriately to experts within the executive branch).

on Congress[178] toward reform suggests that a meaningful increase in legislative oversight of the intelligence community will not occur in the near future.

Leaks like that of Snowden, combined with rigorous and responsible press coverage, can provide some level of constraint on and accountability over intelligence community activity.[179] However, the tendency toward public inertia and the possibility that democratic institutions will not actually provide a substantive check on the surveillance apparatus[180] suggest weakness in relying solely on this approach. Further, the crackdown on leaking and the treatment of whistleblowers as criminals, even prior to Snowden's disclosures,[181] combined with heightened security measures, means that reliance on leaking as a meaningful structural check is misplaced.

Tinkering with the structure inside of the NSA also seems to achieve more in terms of burnishing a veneer of accountability rather than creating genuine oversight. It is hard to understand how various proposed reforms, such as appointing a civilian to oversee the NSA[182] or creating a more adversarial internal review process within the NSA,[183] would increase accountability and transparency. For the executive branch, it seems more likely that pressure from business and corporate interests trying to retain consumer business[184] may shape NSA parameters for mass data collection and domestic surveillance in some respects,[185] but will

---

[178] Some have argued that public pressure on Congress and the executive branch can itself constitute a constraint on intelligence community activity. *See generally* JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11 205–43 (2012) (arguing that an internal oversight process, an active press, leaked information that energized public critique, and other factors created a "presidential synopticon" that effectively restrained executive branch decision-making). Some challenged Professor Goldsmith's argument on grounds that it did not provide a structural, reliable, ex ante constraint on executive power. *See* Neal Kumar Katyal, *Stochastic Constraint*, 126 HARV. L. REV. 990 (2013) (finding the ex post constraints offered by Goldsmith to be lacking in effectiveness and constitutional structural integrity); *cf.* Jack Goldsmith, *A Reply to Professor Katyal*, HARV. L. REV. F. (Feb. 2013), http://www.harvardlawreview.org/issues/126/february13/forum_1004.php#_ftnref16 (defending his original thesis on the grounds that such informal ex post constraints were anticipated and understood by the framers of the U.S. Constitution).

[179] *See generally* Sagar, *supra* note 107.

[180] *See* Glennon, *supra* note 26, at 13–15.

[181] *See* Sue Halpern, *Partial Disclosure,* N.Y. REVIEW OF BOOKS (July 10, 2014), http://www.nybooks.com/articles/archives/2014/jul/10/glenn-greenwald-partial-disclosure/. Halpern offers some detail on how NSA whistleblowers from several years prior to Snowden's disclosures did not have their concerns taken seriously but were subjected to FBI interrogation, searches of their homes, and/or threats of prosecution. As such, Halpern argues, Snowden acted as he did after being "[s]tymied by an unresponsive bureaucracy, seeing the fate of earlier NSA whistleblowers, and finding no adequate provisions within the system to challenge the legality of government activity if that activity was considered by the government to touch on national security." *Id.*

[182] *See* Spencer Ackerman, *White House Considers Appointing Civilian NSA Chief amid Calls for Reform*, GUARDIAN (Nov. 11, 2013, 12:39 PM), http://www.theguardian.com/world/2013/nov/11/white-house-nsa-civilian-director-reform.

[183] *See* Fox News, *Capitol Hill Republicans Disagree on Future of NSA Spying, King Attacks Paul*, FOX NEWS (Aug. 18, 2013), http://www.foxnews.com/politics/2013/08/18/capitol-hill-republicans-disagree-future-nsa-spying-king-attacks-paul/ (arguing that there are "no repercussions" when there is no external review of such programs).

[184] *E.g.*, Claire Cain Miller, *Angry Over U.S. Surveillance, Tech Giants Bolster Defenses*, N.Y. TIMES (Oct. 31, 2013), http://www.nytimes.com/2013/11/01/technology/angry-over-us-surveillance-tech-giants-bolster-defenses.html?hp&_r=0.

[185] Simultaneously, private companies have stepped up efforts to prevent law enforcement and intelligence community access to customer data and transmissions in an effort to reassure customers as

likely not lead to institutional or structural changes as to the government's approach to surveillance without additional pressure from the public.

One promising move with regard to oversight and transparency has been the establishment and staffing of the Privacy and Civil Liberties Oversight Board (PCLOB).[186] This board, tasked with assessing many aspects of the government's national security apparatus both for efficacy and for potentially unnecessary incursions into civil liberties, has a broad mandate and, compared with many national security decision makers, significant independence from the executive branch.[187] Retrospectively, the PCLOB has, among other things, issued the highly critical report of the NSA Metadata Program in January 2014 that led to further public pressure on the Obama administration to curtail this program; it is promising that the PCLOB's prospective agenda includes further analysis of various surveillance programs.[188] However, the PCLOB's potential influence in protecting civil rights may be limited by its position: The PCLOB is an advisory body that analyzes existing and proposed programs and possibly recommends changes, but it cannot mandate that those changes be implemented. The ability to have a high level of access to information surrounding counterterrorism surveillance programs and to recommend changes in such programs is important and should be lauded, but over-reliance on the PCLOB's non-binding advice to the intelligence community to somehow solve the accountability and transparency gap with regard to these programs would be a mistake.

For example, on prospective matters, it is likely that intelligence agencies would consult the PCLOB only if the agency itself considers the issue being faced new or novel, as the NSA metadata program was labeled prior to its inception. In such cases, decision makers within an agency generally ask whether the contemplated program is useful or necessary, technologically feasible, and legal. If all three questions are answered affirmatively, the program can be implemented. Now that the PCLOB is fully operational, it seems likely that if a contemplated program is considered new or novel, an intelligence agency would consult the PCLOB at some stage of this process for its guidance on implementing the program. This nonpartisan external input may improve self-policing within the

---

to their privacy, an effort that has prompted law enforcement and intelligence community concerns in the United States and elsewhere. *See* Brian Naylor, *Apply Says iOS Encryption Protects Privacy; FBI Raises Crime Fears*, NPR (Oct. 8, 2014 at 5:17 PM), http://www.npr.org/blogs/alltechconsidered/2014/10/08/354598527/apple-says-ios-encryption-protects-privacy-fbi-raises-crime-fears (detailing ways in which Apple's operating system prevents warrantless searches of data kept on a smartphone, and the FBI's consternation at this technology); Robert Hannigan, *The Web Is a Terrorist's Command-and-Control Network of Choice,* FIN. TIMES (Nov. 3, 2014 at 6:03 PM), http://www.ft.com/intl/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3I5nuL36a (opinion of the head of GCHQ as to how terrorists can exploit social media and internet sites maintained by U.S. companies).

[186] Establishing the Privacy and Civil Liberties Oversight Board (PCLOB) was a recommendation of the 9/11 Commission Report. The PCLOB was statutorily authorized in 2007, but only became operational and fully staffed in late 2013 and early 2014, months after the Snowden disclosures. *See* GARRETT HATCH, CONG. RESEARCH SERV., RL34385, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD: NEW INDEPENDENT AGENCY STATUS (2012) (describing the establishment of the PCLOB).

[187] *See* Michael J. Glennon, *National Security and Double Government*, 5 HARV. NAT'L SECURITY J. 1, 9 (2014) (listing the numerous national security officials who served in multiple posts in both Republican and Democratic administrations).

[188] *See PCLOB Announces Its Short-Term Agenda*, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD. (Aug. 7, 2014), *available at* http://www.pclob.gov/newsroom/20140807.html (including assessment of E.O. 12,333 and other surveillance authorities).

intelligence community and help intelligence agencies avoid implementing controversial programs or, even if implemented, set better parameters around new programs.[189]

If the PCLOB is able to exert some degree of soft power in influencing national security decision-making, then the judiciary represents hard power that could be used to force the protection of civil liberties where it might not otherwise occur. The FISC should be reformed to include a public advocate lobbying on behalf of privacy concerns, making the process genuinely adversarial and strengthening the FISC against charges that it merely rubber stamps applications from the intelligence community.[190] Article III courts need to follow the lead of Judge Leon in *Klayman* in conceptualizing privacy as broad and defensible, even in a world where electronics-based communication is dominant and relatively easy for the government to collect. If the judicial defense of privacy were combined with the possibility of liability for violations of that privacy, it is likely that this would incentivize increased self-policing among the members of the intelligence community. The creation of an active PCLOB and a more adversarial process before the FISC will not provide a perfect solution to the dilemmas posed by the government's legitimate need for secrecy and the protection of the public against potential abuse. Yet because these changes are institutional and structural, they are well-placed to improve the dynamic between the intelligence community, oversight mechanisms, and the public.

CONCLUSION

Genuine accountability should not depend on the chance that an unauthorized and illegal leak will occur. In the comparative example of the United Kingdom, engagement with a European Union energized with a commitment to increase privacy protections, along with domestic parliamentary oversight, provide two potential avenues for increased constraint on surveillance. In India, the parliament and the courts historically enabled, not constrained, the intelligence community. Whether that stance will continue as the government's technological capabilities increase is yet to be seen.

Domestically, it could be argued that the types of reform recommended here to improve actual accountability and transparency over programs like the NSA Metadata Program are overkill: They involve multiple branches of government, the PCLOB, and the public. However, much of the accountability apparatus that has been in place was dormant until the Snowden disclosures, and would have remained passive without those disclosures. A multi-faceted, long-term, structural approach

---

[189] In other national security contexts, it is clear that government officials would refuse to engage in potentially illegal behavior without the "golden shield" of protection against civil and criminal liability. *See* Sudha Setty, *No More Secret Laws: How Transparency of Executive Branch Legal Policy Doesn't Let the Terrorists Win*, 57 U. KAN. L. REV. 579, 604 (2009) (describing how CIA interrogators required comfort letters from the Office of Legal Counsel protecting them against liability before engaging in the torture of detainees); *see also* Glennon, *supra* note 26, at 78 (President Bush's decisions with regard to initiating and suspending metadata collection were dependent on Office of Legal Counsel guidance at the time).

[190] *See* ANDREW NOLAN ET AL., CONG. RESEARCH SERV., R43260, REFORM OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS: INTRODUCING A PUBLIC ADVOCATE (2014) (describing the constitutional and other parameters that would be considered in establishing a FISC public advocate).

to improving transparency and accountability—one that involves at a minimum the courts and the PCLOB, but hopefully Congress, the executive branch, and the public as well—improves the likelihood of sustained and meaningful accountability as new surveillance capabilities are developed and implemented.