SURVEILLANCE AND THE INVERSION OF DEMOCRATIC TRANSPARENCY

Sudha Setty

Introduction

The traditional structure of a democracy includes the people who have the right to live largely private lives, and a government that has few secrets because it is empowered by the people to act in their name and its workings are transparent to the government’s constituents. Yet national security-related surveillance and the secrecy with which it is conducted invert the democratic structure of transparency in ways that corrode the polity and its underlying assumptions.

In the United States, post-9/11, fear of terrorism has influenced not only substantive laws and policies but also the manner in which they are constructed. The results are evident in the laws governing mass data collection and retention programs—such as those made public by former National Security Agency (NSA) contractor Edward Snowden from 2013 onward. Vaguely worded laws have become enabling and justifying mechanisms for intrusive data collection programs that are largely kept secret from the public. The unwillingness or political inability of the Obama administration and Congress to consider curtailing these controversial and arguably unconstitutional surveillance programs until a high-profile leak occurred suggested that asserting significant democratic control over such programs, once implemented, was unlikely. Simultaneously, the unwillingness of the judiciary to allow for litigation on secret surveillance programs until the Snowden leak occurred suggested the lack of a judicial avenue toward transparency as well. This dynamic has become more pronounced under the Trump administration: secrecy claimed over various government programs has increased, and the ability to marshal any meaningful accountability over those programs has diminished significantly.

Absent a multifaceted response in which transparency of the law is considered a priority by Congress, the judiciary and the public, it seems unlikely that the United States will be able to address the issue of democratic transparency effectively from a structural standpoint.

This chapter addresses the issue of secret surveillance as an inversion of democracy. First, it considers recent debate over secret surveillance programs and discusses the role that leaked information has played in giving the public greater understanding of what kinds of surveillance programs exist. Second, it considers the sometimes vague and opaque legal authorities
that have been relied upon in the post-September 11 context to justify surveillance. Third, it argues that national security surveillance, when justified in secret and without adequate accountability measures in place, undermines the transparency norms that a liberal democracy demands.

2.1 The current debate on secret surveillance

The terrorist attacks of September 11, 2001 led to a significant increase in U.S. domestic and foreign surveillance efforts, partly as a response to the perception that intelligence agencies failed to gather intelligence that could have prevented the attacks. There was significant disagreement within the U.S. government and intelligence community as to whether the failure was due primarily to existing legal constraints, or to an inability to analyze the available intelligence accurately and thoroughly. The 9/11 Commission agreed with the latter view, concluding that whatever pre-9/11 failures the intelligence community suffered, they were not attributable to a lack of legal authority to collect data and to conduct surveillance. Nonetheless, political and public pressure to prevent another large-scale terrorist attack on U.S. soil led to the loosening of legal and policy constraints on intelligence gathering, despite an understanding of the potential adverse effects of such loosening on civil liberties and constitutional rights.

As part of this shift, broad programs were implemented without significant understanding by the public and, at times, by members of Congress, as to their scope and details. As discussed below, the secret collection and storage of domestic telephony and internet metadata and the collection and content searches of substantial amounts of foreign telephone and internet communications was arguably statutorily authorized, giving the intelligence community a much larger “haystack” of information within which to investigate possible emerging and ongoing terrorist threats. For many years, critics of these expanded statutory authorities were unable to secure significant and lasting victories in curtailing surveillance powers, either through judicial action or legislative initiative. One of the key reasons behind this inability to challenge surveillance effectively was the secret nature of the programs: without public knowledge of the extent to which surveillance existed, Congress was unable or unwilling to act, and plaintiffs looking to challenge domestic surveillance in court were almost uniformly found to lack standing to bring their claims.

The public debate shifted in June 2013, when then-NSA contractor Edward Snowden began revealing classified documents as to the scope of NSA surveillance on foreign and U.S. persons, with the stated purpose of prompting public scrutiny and debate over the programs. Snowden revealed, among 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, 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 (the “NSA Metadata Program”). One of Snowden’s stated intents in revealing the details of this program—its secret operations, broad scope, lack of particularized suspicion, and lengthy duration of data retention—was to allow “the public to be able to have a say in how they are governed.” In other words, Snowden sought, at least in part, to restore democratic transparency with regard to a program that was largely unknown and unknowable to the public prior to his disclosures.

If increasing democratic discourse and discussion of potential accountability was one of Snowden’s objectives, then this was achieved to some extent by public demands for better oversight of the NSA. The Obama administration initiated various review mechanisms;
Congress discussed and debated its oversight role;\textsuperscript{16} and former judges on the Foreign Intelligence Surveillance Court (FISC), tasked with determining whether government requests for surveillance authority should be authorized, weighed in on matters of secrecy and government accountability.\textsuperscript{17}

\textbf{2.2 National security’s domestic surveillance authorities}

The legal architecture constructed to support arguments as to the domestic authorization of the NSA Metadata Program was extensive.\textsuperscript{18} A significant number of laws—such as the 2001 Authorization for the Use of Military Force,\textsuperscript{19} provisions of the USA PATRIOT Act ("Patriot Act"),\textsuperscript{20} the Protect America Act and the FISA Amendments Act of 2008\textsuperscript{21}—were enacted by Congress and interpreted by the NSA as providing ample statutory authority for the capture and storage of data.\textsuperscript{22} Compounding these statutory authorities, the executive branch likely sought its own non-public legal guidance in the form of secret legal opinions from the Office of Legal Counsel\textsuperscript{23} and other Department of Justice memoranda defending the legality and efficacy of the surveillance program.\textsuperscript{24}

After the Snowden disclosures began, public pressure mounted for the Obama administration and Congress to take action to better protect individual privacy rights from government overreaching. This led to the passage of the USA FREEDOM Act in mid-2015 that curtailed the scope of metadata collection starting in December 2015.\textsuperscript{25} When the USA FREEDOM Act came into effect, it mandated that intelligence agencies such as the NSA stop gathering and storing metadata for their own use without further judicial oversight. Instead, when an intelligence agency needs to gather metadata on an individual or group, it must seek it from the telecommunications companies that store such data, and only after obtaining an individualized warrant from the FISC to do so.\textsuperscript{26} The USA FREEDOM Act also encourages the publication of FISC opinions under some circumstances,\textsuperscript{27} and gives FISC judges the opportunity to appoint amici curiae to argue against the government’s request for surveillance authorities,\textsuperscript{28} thereby offering, in some circumstances, an adversarial process before that court. As discussed below, the Snowden disclosures also encouraged administrative measures, such as the staffing and funding of a Privacy and Civil Liberties Oversight Board, to give advice on whether certain surveillance activities impermissibly infringed on the privacy rights of both U.S. citizens and non-citizens.

Courts also took on a more active role with regard to providing meaningful oversight after June 2013. Prior to the start of the Snowden disclosures, the surveillance and data collection that are part of the NSA Metadata Program were upheld by two forms of relatively weak judicial review. Ordinary federal courts largely refused to hear the merits of cases challenging government surveillance, instead finding that plaintiffs were unable to satisfy the standing requirement,\textsuperscript{29} or dismissed suits at the pleadings stage due to invocations of the state secrets privilege by the government.\textsuperscript{30} The FISC had operated largely in secret and without an adversarial process to contest the government’s arguments. When the U.S. government first sought and received FISC approval for the NSA Metadata Program in 2006, the NSA argued that U.S. national security interests demanded non-public access to vast swaths of data, since one of the “greatest challenges” faced by the government was the identification of potential threats from al Qaeda,\textsuperscript{31} and that individualized data collection would be insufficient to counter the potential terrorist threat.\textsuperscript{32} The government further argued\textsuperscript{33} that it would be insufficient to allow telecommunications companies to hold the metadata and have the government make individualized metadata requests, since the possibility of the companies not saving the data for a sufficiently long period of time might jeopardize intelligence-gathering

\textsuperscript{25}Sudha Setty

\textsuperscript{30}
efforts.\textsuperscript{34} The government’s justification for the vast, non-public collection of data it was seeking was simple and powerful: “the government’s interest is the most compelling imaginable: the defense of the Nation in wartime from attacks that may take thousands of lives.”\textsuperscript{35} This argument was convincing to the FISC. Not only did it approve the NSA Metadata program, but it overwhelmingly acquiesced to government requests for surveillance authorities over the years.\textsuperscript{36}

After the Snowden disclosures began in June 2013, however, the government’s justification for the NSA Metadata Program shifted away from identifying al Qaeda as a near-existential threat to simply stating that bulk metadata collection was still a necessary part of the U.S. counterterrorism strategy.\textsuperscript{37} Cases litigated after June 2013, but prior to the USA FREEDOM Act taking effect, suggest that the judicial deference offered to the government in many previous counterterrorism cases softened in some jurisdictions in favor of a somewhat more rights-protective stance, particularly in light of public attention and critique of the NSA Metadata Program, as well as a reinvigorated judicial embrace of the privacy protections embodied in the Fourth Amendment.\textsuperscript{38} One federal circuit court continued the deferential posture of dismissing suits seeking to challenge the government’s collection of their metadata at an early stage,\textsuperscript{39} and the FISC validated its own previous authorization of bulk metadata collection.\textsuperscript{40} Yet, for other courts, the issue of the secret surveillance authorities was anathema\textsuperscript{41} to the idea of democracy and, therefore, could not be legal. One court rejected the Obama administration’s contention that the NSA Metadata Program must be legal because it was being run under the auspices of Section 215 of the USA PATRIOT Act, stating simply that “Congress cannot reasonably be said to have ratified a program of which many members of Congress—and all members of the public—were not aware.”\textsuperscript{42}

The Supreme Court, although not weighing in on the NSA Metadata Program per se, has made clear in the years since the passage of the USA FREEDOM Act that it, too, is wary of government surveillance conducted in secrecy and without appropriate accountability mechanisms in place. Perhaps the most prominent recent example of this dynamic is the 2018 case of \textit{Carpenter v. United States},\textsuperscript{43} which held that historical cell tower data that could pinpoint the location of individuals carrying cell phones cannot be accessed by law enforcement without a judicial warrant, and that the appropriate standard for getting a warrant is a showing of probable cause. Although U.S. courts have been largely deferential to law enforcement and intelligence agency claims that any limitation on their ability to collect data might lead to another large-scale terrorist attack, the \textit{Carpenter} court resisted, acknowledging the need for limits as to what the government can surveil, as well as for accountability.

### 2.3 Broad, secret surveillance inverts democratic transparency

The post-9/11 government use of extremely intrusive surveillance technology, along with the secrecy of these programs from the public, resulted in an inversion of the transparency on which democracy ordinarily relies.\textsuperscript{44} The deployment of powerful and intrusive surveillance technology essentially renders citizens of liberal democratic nations, who are normally afforded the right to privacy, transparent to the government. The scope of government surveillance and the legal basis on which that surveillance has been justified has been opaque to the public absent the benefit of leaked information. These two forces combine to create a Panopticon-like surveillance regime in which the government has the ability to watch and collect vast amounts of data on the population secretly. Since the populace is unable to ascertain the parameters of when the surveillance might occur, they must operate under the
belief that all of their telephonic and internet activity may be examined by the government at any time.\textsuperscript{45}

Particularly since the early years of the Cold War, the public, Congress, and the judiciary have ceded large swaths of security-related decision-making authority to the executive branch,\textsuperscript{46} often allowing security-related decisions to be made in secret, without the traditional transparency on which democracy relies.\textsuperscript{47} Despite this shift in policy-making authority, security policies that have led to broad, secret surveillance and data collection have been historically viewed by politicians and judges as antithetical to the democratic foundation of the United States. Several important examples stem from the contentious discussions around secret surveillance and democratic transparency in the 1970s. When the Supreme Court decided to uphold a warrant requirement for domestic surveillance in the 1972 \textit{Keith} case, the tenor and language of the opinion focused on the need to uphold the privacy rights of Americans as a bulwark of a democratic society: “Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of government action in private conversation. For private dissent, no less than open public disclosure is essential to our free society.”\textsuperscript{48}

In 1976, the Church Committee’s investigations into the National Security Agency and its domestic intelligence-gathering operations yielded the conclusion that:

Americans have rightfully been concerned since before World War II about the dangers of hostile foreign agents likely to commit acts of espionage. Similarly, the violent acts of political terrorists can seriously endanger the rights of Americans. Carefully focused intelligence investigations can help prevent such acts.

But too often intelligence has lost this focus and domestic intelligence activities have invaded individual privacy and violated the rights of lawful assembly and political expression. Unless new and tighter controls are established by legislation, domestic intelligence activities threaten to undermine our democratic society and fundamentally alter its nature.\textsuperscript{49}

Further, when Congress debated the enactment of the Foreign Intelligence Surveillance Act of 1978, a significant amount of legislative discourse focused on the extent to which warrantless surveillance might undermine democratic values.\textsuperscript{50} The concern centered on the corrosion of democracy that occurs when the scope of the government’s actions and legal authority ceases to be transparent to the public, thereby unmooring the government’s actions from any form of democratic accountability. The extent to which Congress could function as a democratically elected source of constraint on the intelligence community was stifled by the structure of FISA, which vested sole control in the Foreign Intelligence Surveillance Court, with its closed hearings and secret body of law.\textsuperscript{51}

In the post-9/11 era, the same kind of deliberation and debate should have occurred; but a combination of factors—including genuine concerns for national security, broad claims of executive authority, an overly deferential judiciary, and political fear of seeming to be “soft on terror” during an election cycle—stifled essential debate on questions of secret law and the undermining of the rule of law. Instead, the enormous technological capabilities available to the government, the murky statutory authority on which surveillance programs are predicated, the secrecy of the intelligence community, and the lack of access to FISA decisions rendered the Panopticon complete.

In this context, democratic control mechanisms ordinarily available are not effective in restoring transparency over the surveillance apparatus. First, the public is not given enough
information to create informed opinion as to the types of surveillance policies adopted and utilized by the government. Therefore the public cannot be realistically expected to serve as a source of democratic accountability. Instead the public relies on leaks such as those regarding the Terrorist Surveillance Program in 2005 and the disclosures by Edward Snowden in 2013 and onward for specific information about the broad surveillance measures being taken unannounced in the name of national security. These leaks engaged the public in debate, and have led to some reforms that limited surveillance and data collection authority. Still it is notable that such reforms under the George W. Bush and Obama administrations stemmed from the executive branch first, with Congress following and curbing programs to parameters with which each administration felt comfortable. Even then, it was clear that ad hoc leaking of classified information was not an adequate substitute for a structural means by which democratic accountability can exist. Given the Obama administration’s crackdown on leaking and the treatment of whistleblowers as criminals, as well as heightened security measures in the wake of leaking, reliance on leaking as a means of achieving democratic discourse, and as a meaningful check on government actions, proved to be misplaced. Under the Trump administration, adherence to democratic norms and values has been largely abandoned, leaks continue to be prosecuted aggressively, and secrecy over national security matters has grown significantly. Reliance on the administration to maintain transparency would be misplaced, and reliance on leaks does not serve as a substitute for genuine accountability.

Ideally, Congress could serve as another possible means of exercising oversight and democratic control. Relying on Congress is an appealing option to prevent disclosure of sensitive material or to discipline unwarranted surveillance in an effort to prevent disclosure of sensitive or classified national security information. But Congress has been hamstrung by its inability and unwillingness to make informed decisions with regard to surveillance programs. First, absent high-profile leaks, Congress itself has not been particularly well-informed by more than one administration with regard to the parameters of surveillance programs: limitations on briefings to certain congressional committees, misleading responses to congressional oversight hearings, and the inability of members of Congress to consult with staff on certain programs create an information deficit that hampers effective oversight.

Second, even when information is made available, most members of Congress do not avail themselves of opportunities to improve their understanding of surveillance programs utilized by the intelligence community. Third, and relatedly, it may be politically expedient for Congress to exercise willful blindness when it comes to the more controversial aspects of surveillance programs; if those programs become public later and are met with anger or discontent, as with the case of the NSA Metadata Program, members of Congress can use plausible deniability as political cover and lay blame on the administration and the intelligence community. This arguably explains some of the congressional furor over the NSA Metadata Program, and part of the righteous impetus behind the USA FREEDOM Act. Fourth, under certain circumstances Congress can later assert itself in a limited fashion as a rights-protective body. As with the USA FREEDOM Act, this may be based largely on information provided through the administration and through leaking, and/or with the approval of the administration.

As an alternative to reliance on somewhat unreliable democratic controls, two non-democratic mechanisms exist as potential means of restoring a semblance of democratic transparency: the judiciary and independent oversight mechanisms operating within an administration. As discussed above, ordinary federal courts and the FISC have been largely reluctant to engage with matters administrations deem to involve national security secrets.
Relying solely on administrations to self-police seems to have been ineffective in curtailing numerous practices that undermine the rule of law, including the development of secret law and policy governing national security and related matters. By contrast, the Privacy and Civil Liberties Oversight Board (PCLOB), born out of a 9/11 Commission recommendation, is one potential avenue for accountability over some national security matters.

The PCLOB’s mission is to assess aspects of the government’s national security programs for efficacy and for potentially unnecessary incursions into civil liberties. The PCLOB has some independence from the executive branch. Initially, its promise to curb potential abuses seemed significant. With regard to the NSA Metadata Program, the PCLOB issued a highly critical report in January 2014 that added pressure on the Obama administration to curtail this program, and encouraged congressional debate on what eventually passed as the USA FREEDOM Act. Prospectively, it seemed possible that an intelligence agency would consult the PCLOB if the agency itself considered an issue it faced to be new or novel (the NSA Metadata Program was labeled novel 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, and only implement a program if all three questions are answered affirmatively. If a contemplated program is considered new or novel by an intelligence agency, a best-case scenario for maintaining government accountability would involve consultation with the PCLOB at some stage of the process. This nonpartisan external input may improve self-policing within the intelligence community, help intelligence agencies avoid implementing controversial programs, or, even if such programs are implemented, set better parameters for new programs. Because the PCLOB issues public reports, this non-democratic institution offers the possibility of restoring some level of transparency to inform the public about the types of surveillance programs the government operates.

Still, the Board’s potential influence in protecting civil liberties is based on soft power. Its resources are limited by its position as an advisory body: it cannot mandate any changes. 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 reliance on the PCLOB’s non-binding advice to the intelligence community to fully resolve the accountability and transparency gap with regard to these programs would be a mistake. The PCLOB’s soft power is further limited when the Board is insufficiently resourced to do its work. The PCLOB was fully staffed in 2013, after the Snowden disclosures were made, at which point it began to investigate and produce significant reports. In 2017 PCLOB staff shrank from its full complement of five board members to one. Only in 2019, after several years of dormancy, was the PCLOB again fully staffed and thus able to set an agenda for new investigations and oversight efforts.

Conclusion

The idea that secret law is anathema to a liberal democracy is well-established in the United States. Yet transparency with regard to national security surveillance programs has been and will continue to be a challenge. Particularly at times of heightened stress over national security, as in the wake of a large-scale terrorist attack, the political and public imperative shifts to further empowering the surveillance apparatus without transparency requirements and other safeguards against potential abuse that would be considered more carefully when governments are not on an emergency or war footing. Like other nations, the United States has depended on leaking as a form of unauthorized transparency to engage the public in
debate over improved accountability measures. However, unlike other countries that struggle with similar issues in terms of counterterrorism powers and the need for democratic transparency, the absence of supranational or effective international controls upon the United States puts it in a more precarious situation in that it has an even greater dependence on leaking to force a measure of transparency. Under these circumstances it becomes all the more necessary for each branch of the U.S. government to engage more fully and proactively in matters of national security surveillance in an effort to provide accountability and transparency that would otherwise be lacking but for the leak of government information. The unwillingness and inability thus far of Congress and the judiciary to do so represent a systemic failure to safeguard the democratic value of transparency. Passage of the USA FREE-DOM Act, the restaffing of the PCLOB in 2019, and recent jurisprudence that indicates an interest in curbing government surveillance authorities suggest the possibility of a future that values transparency more fully. The efficacy and durability of those developments are yet to be seen.

Notes

1 Some elements of this chapter are drawn from a previous work: Sudha Setty, Surveillance, Secrecy, and the Search for Meaningful Accountability, 51 STAN. J. INT’L L. 69 (2015) © Sudha Setty 2015. I deeply appreciate the comments and suggestions offered on this project by participants at workshops at the University of Connecticut School of Law and the University of South Carolina School of Law, both held in March 2015. I am grateful to Matthew H. Charity, Richard S. Kay, Mark Weston Janis, Molly Land, Peter L. Lindseth, the late Robert Prasch, Wadie E. Said and Falguni A. Sheth for thoughtful comments and insights. Finally, I thank Ryan O’Hara and Joseph Greenhalgh for fine research assistance.


3 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”).

4 See Testimony of Professor Stephen J. Schulhofer Before the National Commission on Terrorist Attacks Upon the United States 1 (Dec. 8, 2003), 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”).

5 The National Commission on Terrorist Attacks Upon the United States is also known as the “9/11 Commission.”


7 The telephony metadata authorized for collection is defined as: “includ[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 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 Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], 3 n.1 (FISA Ct. 2013), www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf.

8 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. at § 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 alteration. See David Kravets, Lawmakers Punt Patriot Act to Obama, WIRED (Feb. 26, 2010), www.wired.com/2010/02/lawmakers-renew-patriot-act/.

9 See Gil Press, The Effectiveness of Small vs. Big Data Is Where the NSA Debate Should Start, FORBES. (June 12, 2013), 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).

10 E.g., Clapper v. Amnesty Int’l, No. 11–1025 (U.S. Feb 26, 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.

11 Of course, the U.S. intelligence community has engaged in numerous programs involving warrantless surveillance, and this chapter only addresses the bulk metadata collection that was 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 chapter. 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.


16 See Senator Ron Wyden & Senator Mark Udall, Wyden, Udall Statement on Reports of Compliance Violations Made Under NSA Collection Programs, RON WYDEN SENATOR FOR OREGON (Aug. 16, 2013), 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).

17 E.g., See Carol Leonnig, Court: Ability to Police U.S. Spying Program Limited, WASH. POST (Aug. 15, 2013), www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c84a4-05cd-11e3-a07f-49dcd7417125_story.html (quoting Judge Reggie Walton as lamenting 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”). Judge James Carr, A Better Secret Court, N.Y. TIMES (July 22, 2013), www.nytimes.com/2013/07/23/opinion/a-better-secret-court.html.

18 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.
Surveillance and democratic transparency

20 See Patriot Act, Pub. L. No. 107–56, § 218, 115 Stat. 287 (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.
23 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).
24 See Weich, supra note 22 (including Justice Department analysis of the legislative authority supporting the NSA’s bulk metadata collection program).
30 See Al-Haramain Islamic Found. v. Obama, 705 F.3d 845 (9th Cir. 2012).
32 Id. at 1–2.
33 Some arguments for the NSA Metadata Program that were heard by the FISC in 2006 have yet to be disclosed. See id. at 10–11 (a heavily redacted portion of the NSA Memo).
34 Id. at 9–10.
35 Id. at 3.
36 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), http://fas.org/irp/agency/doj/electronic-spying.html.
38 See, e.g., Klayman v. Obama, Civ. No. 13–851 (D.D.C. Nov. 9, 2015) (holding that the NSA Metadata Program violates the Fourth Amendment); 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).
40 In re Application of the FBI for an Order Requiring the Production of Tangible Things, Nos. BR 15–75, Misc. 15–01 (FISA Ct. June 29, 2015) (same).
41 ACLU v. Clapper, 785 F.3d 787, 792 (2d Cir. 2015) (holding that the NSA Metadata Program was not statutorily authorized); Klayman v. Obama, F. Supp. 2d 1 (D.D.C. 2013) (finding that the Section 215 metadata collection program was illegal).
42 ACLU v. Clapper, 785 F.3d at 819.
44 Although this chapter focuses on the NSA Metadata Program, the inversion of democratic transparency exists with regard to other federal surveillance programs, as well as the surveillance efforts of state and local police departments that now have access to powerful surveillance technology because of federal government largess. See Matt Richtel, A Police Gadget Tracks Phones? Shh! It’s Secret, N.Y. TIMES (March 16, 2015), http://nyti.ms/18Qewm5 (noting that local police departments have been purchasing powerful surveillance technology using Homeland Security grants, and that purchase of the technology was predicated on municipalities agreeing not to demand access to detailed information about the technology and signing broad non-disclosure agreements).
The Panopticon—a plan for a prison proposed by utilitarian philosopher Jeremy Bentham in the late 18th century, in which prisoners could not be aware of when they were being watched by guards and, therefore, would always feel pressured to act as though their captors were watching them—was invoked by 20th-century philosopher Michel Foucault as an example of the way in which governments seek to categorize and control their subjects. See Michel Foucault, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 135–48 (Vintage Books 1995).

See Aziz Rana, Who Decides on Security? 44 CONN. L. REV. 1419 (2012). Rana argues that this post–World War II posture marked a significant change from the democratic grounding of security-related decisions in the early Republic and 19th century. Id. at 1442–43.


United States Senate, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Intelligence Activities and the Rights of Americans, Book II, at 1 (April 24, 1976).


Id. at 46–47.


In February 2015, the Director of National Intelligence announced new limits to the scope of Section 215 surveillance and intelligence-gathering that largely reflected the type of limitations suggested by President Obama in 2014. See ODNI General Counsel Robert Litt’s As Prepared Remarks on Signals Intelligence Reform at the Brookings Institute, Feb. 4, 2015, http://icontherecord.tumblr.com/post/110632851413/odni-general-counsel-robert-litts-as-prepared.


See Sue Halpern, Partial Disclosure, NEW YORK REVIEW OF BOOKS (July 10, 2014), 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.”


E.g. Kate Oh, Trump’s Year of Secrecy, justsecurity.org (Dec. 12, 2017), www.justsecurity.org/48932/trumps-year-secrecy/.

See Weich, supra note 22, at 25.

This information was gleaned from interviews with current and former officials within the NSA; notes on file with the author.

See Rana, supra note 46, at 1422 (arguing that Congress tends to cede decision-making power back to the executive branch on national security matters, giving the administration little oversight but providing a “constitutional imprimatur” to security programs).


In some national security contexts, it has been clear that government officials would refuse to engage in potentially illegal behavior without the “golden shield” of protection against civil and criminal liability. See Glennon, supra note 23, 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).