Hastings Law Journal

Volume 66 | Issue 1 Article 1

12-2014

Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden

Peter Margulies

Articles

Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden

PETER MARGULIES*

This Article outlines a dynamic conception of national security surveillance that justifies programs disclosed by Edward Snowden but calls for greater transparency and accountability in the wake of Snowden's revelations. The dynamic conception supports the legality of section 215 of the USA Patriot Act and section 702 of the Foreign Intelligence Surveillance Act ("FISA"), programs that received informed input from all three branches of government. Each program is part of a long democratic experiment in the integration of secrecy, deliberation, and strategic advantage that dates to the Constitution's framing. Both programs reflect Congress's concern that intelligence collection be sufficiently agile to keep up with evolving threats. The Foreign Intelligence Surveillance Court ("FISC") required that both programs use technology not only to collect data, but also to prevent unduly intrusive government use of that data. However, even though both section 215 and section 702 were legal in their pre-Snowden iterations, changes are now necessary to ensure the programs' legitimacy.

Legislation sponsored by Senator Patrick Leahy modifies section 215 by leaving private data in the hands of telecommunications companies and authorizes the FISC to appoint amici to represent the public interest. On the FISC process front, the Leahy bill is a welcome first step, but does not go far enough. A more robust public advocate whose participation does not require permission by the FISC would provide a more meaningful check on the government. This Article argues that a more robust public advocate could withstand constitutional objections based on Article III and the Appointments Clause of the Constitution, and enhance domestic and international faith in the FISC's deliberations.

---

* Professor of Law, Roger Williams University School of Law. B.A. 1978, Colgate University; J.D. 1981, Columbia Law School. I thank reference librarians Nan Balliot and Emilie Benoit for their expert assistance, and Joe Landau, David Pozen, and Ben Wittes for comments on a previous draft.

TABLE OF CONTENTS

INTRODUCTION 3
I. THE STATUTORY FRAMEWORK 11
A. SECTION 215 11
1. *Text and Case Law* 11
2. *The Uses of Metadata* 14
B. SECTION 702 17
II. RELEVANCE UNDER SECTION 215: STATUTORY AMBIGUITY AND *CHEVRON* 20
A. DEFINING RELEVANCE DOWN: A TALE OF THREE DICTIONARIES 20
B. METADATA'S CRITICS ON CASE LAW AND LEGISLATIVE HISTORY 21
C. A CONTRASTING VIEW: RELEVANCE AND THE GOVERNMENT'S ROLE 22
D. SUNSET CLAUSES AND THE DYNAMIC CONCEPTION 25
III. THE REASONABLENESS OF THE DYNAMIC CONCEPTION OF SURVEILLANCE UNDER SECTION 215 27
A. DELIBERATION AND SECRECY 28
B. SECRECY IN AMERICAN LAW 30
1. *Secrecy and the Framers* 31
2. *Secrecy and the Courts* 33
3. *Technology, Secrecy, and National Security* 36
C. TECHNOLOGICAL INNOVATION CAN BOTH ENHANCE AND CHECK THE POWER OF SURVEILLANCE 41
IV. METADATA IN PRACTICE: THE 2009 DISCLOSURES REGARDING NONCOMPLIANCE 45
V. THE DYNAMIC CONCEPTION AFTER SNOWDEN 49
A. SECTION 215, METADATA, AND SPECIFIC SELECTION TERMS 50
B. INSTITUTIONAL REFORM AND EXTERNAL CONSTRAINTS 51
1. *The Policy Case for a Public Advocate* 52
2. *The Legal Case for a Public Advocate* 54
a. *The Public Advocate and Article III* 55
i. *Certification and Its Discontents* 55
ii. *Warrants, Article III, and the Lessons of History* 58
b. *The Public Advocate and the Appointments Clause* 62
C. "ABOUT" COLLECTION UNDER SECTION 702 63
D. QUERYING DATABASES FOR DATA INCIDENTALLY COLLECTED ON U.S. PERSONS 67
CONCLUSION 74

INTRODUCTION

As President Obama noted in a January 2014 speech,[1] American leaders' quest for intelligence about adversaries' plans started with Paul Revere's fabled midnight ride in 1775.[2] Public disclosure of Revere's method would have robbed the colonists of a strategic advantage and limited their options in the impending revolution against British rule. Such consequences do not justify unlimited secrecy or unchecked intelligence collection. However, they demonstrate that current efforts to reform intelligence gathering after Edward Snowden's revelations require great care. This Article argues that a dynamic conception of collection and surveillance authorities can pivot toward greater transparency and accountability, while preserving the effectiveness of intelligence programs.

Revere's example sets the stage for important insights about two controversial programs that figured prominently in Snowden's disclosures: the bulk collection of telephony "metadata" under section 215 of the USA Patriot Act,[3] pursuant to orders issued by the Foreign Intelligence Surveillance Court ("FISC"),[4] and the collection of Internet and telephony content under section 702 of the Foreign Intelligence Surveillance Act ("FISA").[5]

With respect to section 215, critics have argued that the FISC erred in finding that the National Security Agency ("NSA") could acquire, albeit with substantial conditions regarding access, the call records of millions of Americans with no connection to terrorism.[6] According to critics, the bulk collection of metadata that the FISC had approved before Snowden's revelations was far too sweeping to be "relevant to an authorized investigation" of international terrorism or foreign

---

1. *See* Barack Obama, President of the United States, Speech on NSA Reforms (Jan. 17, 2014), *available at* 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.

2. Revere advised a fellow patriot in April 1775 to place one lantern in the steeple of Boston's North Church if the British were planning to take a land route to Lexington and Concord to destroy the colonists' arms caches, and two lanterns if the British were planning to cross the Charles River to points north. *See* JAYNE E. TRIBER, A TRUE REPUBLICAN: THE LIFE OF PAUL REVERE 102 (1998) (relating the story of Paul Revere's ride and describing Revere as "an experienced courier and spy").

3. 50 U.S.C. § 1861 (2011).

4. *See, e.g.*, *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Name Redacted by Court], No. BR 06-05, 2006 WL 7137486 (FISA Ct. May 24, 2006).

5. 50 U.S.C. § 1881a (2011).

6. *See* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 821 (2014); Marty Lederman, *The Kris Paper, and the Problematic FISC Opinion on the Section 215 "Metadata" Collection Program*, JUST SECURITY (Oct. 1, 2013, 5:25 PM), http://justsecurity.org/2013/10/01/kris-paper-legality-section-215-metadata-collection/; *cf.* Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1754–58 (2014) (noting critics' contentions that the FISC has not adequately constrained the executive branch).

intelligence activity under section 215.[7] Critics have asserted that the FISC should have employed a far narrower definition of relevance that precluded bulk collection. Regarding section 702, critics have argued that the FISC erred in permitting collection of content "about" targets, instead of limiting collection to communications to and from targets.[8] In addition, critics have been troubled by the FISC's use of search terms related to U.S. persons to query data that was collected pursuant to statutory authorization of foreign surveillance.[9] On a broader theoretical level, NSA critics argue that the secrecy surrounding the FISC's decisions, the absence of a voice opposing the government's FISC applications, and the lack of public debate in Congress prior to Snowden's revelations corroded decisionmaking and eroded the checks that a public and adversarial process provide.[10]

While the critics' concerns are legitimate, their argument incorporates an unduly stark account of the relationship between government secrecy and two core values in national security surveillance: deliberation and strategic advantage. Secrecy here refers to protection against public disclosure of a program, position, or technique.[11] Deliberation refers to the classical virtue celebrated by the Framers of dialogue on problems and prospective solutions.[12] Strategic advantage refers to the edge that a state obtains over its adversaries, including other states or non-state actors.[13] Critics assert that in conditions of secrecy, strategic advantage assumes outsized importance, leading to the

---

7. *See* 50 U.S.C. § 1861(b)(2) (2011).

8. *See* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y (forthcoming 2015) (manuscript at 58), *available at* http://ssrn.com/abstract=2436418.

9. *Id.*

10. *See* David Cole, *Can Privacy Be Saved?*, N.Y. REV. BKS., Mar. 6, 2014, at 23; Ryan Lizza, *State of Deception: Why Won't the President Rein in the Intelligence Community?*, THE NEW YORKER, Dec. 16, 2013, at 48 (summarizing views of legislative critics of metadata program, particularly Oregon Senator Ron Wyden*); cf.* David E. Pozen, *Deep Secrecy*, 63 STAN. L. REV. 257, 278, 282–83, 287 (2010) (analyzing secrecy's risks and benefits, and cautioning about one aspect of its potential effect on decisionmaking).

11. Pozen, *supra* note 10; Jared Cole, Note, *Historical Gloss and Congressional Power: Control Over Access to National Security Secrets*, 98 VA. L. REV. 1855, 1864–70 (2013).

12. *See* THE FEDERALIST No. 63, at 384 (James Madison) (Clinton Rossiter ed., 1961) (citing the importance of designing institutions such as Senate that will enable "cool and deliberate sense of the community" to prevail over "temporary errors and delusions"); *cf.* HANNAH ARENDT, BETWEEN PAST AND FUTURE 242 (Penguin Books 1977) (1961) (noting process through which "an issue is forced into the open that it may show itself from all sides, in every possible perspective"). The Framers were profoundly influenced by the classical civic humanist tradition of political deliberation that also shaped Arendt's thought. *See* J.L. Hill, *The Five Faces of Freedom in American Political and Constitutional Thought*, 45 B.C. L. REV. 499, 582–83 (2004); Frank Michelman, *Law's Republic*, 97 YALE L.J. 1493, 1495 (1988); Cass R. Sunstein, *Beyond the Republican Revival*, 97 YALE L.J. 1539, 1547–50 (1988).

13. *See* THE FEDERALIST No. 41, *supra* note 12, at 257 (James Madison) (noting risks that arise because the Constitution cannot "chain the ambition or set bounds to the exertions of all other nations," requiring institutional design to respond to those risks).

evisceration of checks and balances that ensure deliberation and protect individual rights.

This Article argues that a "dynamic conception" of surveillance authorities would better integrate secrecy, deliberation, and strategic advantage. The dynamic conception posits that, in the realm of national security surveillance, changing circumstances will affect the appropriate mix of secrecy and deliberation. To qualify as dynamic under this conception, the mix of secrecy and deliberation must involve all three branches of government, not unilateral action by the executive branch. A default position of secret deliberation among the three branches may be appropriate. Because of the rapidly changing nature of external threats, including terrorism, Congress may choose, in the first instance, to limit public disclosure of certain surveillance techniques that give officials the agility to anticipate and meet those threats. Congress can also choose to give a tribunal, such as the FISC, the ability to approve *ex parte* requests from officials to utilize new technologies under a broad legal standard, even without express congressional authorization for such new technologies. At the same time, as part of this shared understanding, Congress will expect that the FISC and the agency conducting collection or surveillance use evolving technology to limit the ways the government uses the data that it has collected. Moreover, this default understanding of the need for secrecy may itself change, as public disclosure, such as Snowden's, diminishes the perceived legitimacy of government surveillance and collection programs. In this new environment, bolstering legitimacy is crucial, and steps that emphasize transparency, external constraints on collection and surveillance, and tailoring surveillance to the public interest will assume priority.

On this view, secrecy and deliberation can be complementary. Deliberation entails choice. In national security and foreign affairs, as the Framers understood, secrecy can expand the menu of options. Public disclosure, in contrast, makes certain options ineffective, removing them from deliberation's reach.[14] Suppose that a diplomat wished to travel to a country that was a long-time adversary to negotiate an agreement. Premature disclosure of the trip would galvanize domestic distrust of the adversary's motives, removing any hope of the agreement.[15] Premature

14. *See* RAHUL SAGAR, SECRETS AND LEAKS: THE DILEMMA OF STATE SECRECY 2 (2013) (noting that "citizens may themselves prefer secrecy when it leads to the execution of worthy policies that cannot otherwise be carried out"); Dennis F. Thompson, *Democratic Secrecy*, 114 POL. SCI. Q., no. 2, 1999, at 182 (without secrecy, some policies "to which citizens would consent if they had the opportunity" "could not be carried out as effectively or at all").

15. *See* SISSELA BOK, LYING: MORAL CHOICE IN PUBLIC AND PRIVATE LIFE 176 (1978) (suggesting that concealing a trip and even issuing a "cover story" claiming that the diplomat was on another mission could be a permissible "white lie," but urging that such tactics be reduced to "an absolute minimum").

disclosure would also neutralize any long-term strategic advantage that an agreement would yield.

Of course, secrecy is not a panacea. In our diplomacy scenario, an enemy might use negotiations as a ruse to buy time for fresh attacks.[16] Wider discussion might have headed off this catastrophe. However, unless we wish to categorically rule out negotiations with long-time foes, we should acknowledge that secrecy will sometimes expand the realm of the possible. One challenge in such cases is to build in checks and balances for a secret process that will replicate the virtues of broad disclosure without its risks. An additional challenge is coping with unauthorized disclosures, like Snowden's, which put a premium on demonstrations of the system's legitimacy. The ultimate test of the dynamic conception is signaling legitimacy while maintaining effectiveness in the wake of such revelations.

We can trace the dynamic conception back to the value placed on secrecy in national security and foreign affairs by the Constitution's Framers. This more favorable view of secrecy has also been a mainstay of judicial precedent, driving decisions on state secrets,[17] government employment,[18] and remedies.[19] The development of increasingly sophisticated technology has accelerated the trend, although courts have tempered this tendency with an awareness of individual rights.[20]

Applied to section 215, the dynamic conception's premise is that Congress intended to keep the statutory relevance standard fluid to accommodate changes in technology, as well as the terrorist threat, while maintaining appropriate privacy safeguards. To fulfill those purposes, Congress drafted section 215 to permit broad collection, narrow but consistent congressional oversight, and judicial imposition of rigorous search protocols that limit NSA access to the bulk telephony database.

---

16. *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 37 (2010) (noting that a violent non-state actor could "pursue peaceful negotiation as a means of buying time to recover from short-term setbacks, lulling opponents into complacency, and ultimately preparing for renewed attacks").

17. *See, e.g.*, Totten v. United States, 92 U.S. 105 (1875) (holding that the need for government secrecy barred a suit by an alleged government agent regarding compensation for a secret mission during the Civil War).

18. *See, e.g.*, Dep't of the Navy v. Egan, 484 U.S. 518, 530 (1988) (holding that the importance of secrecy required limiting the remedies available to an employee seeking to contest discharge that occurred pursuant to loss of required security clearance).

19. *See* Winter v. Natural Res. Def. Council, 555 U.S. 7, 24 (2008) (cautioning against litigation that would result in second-guessing "complex, subtle, and professional decisions as to the composition, training, equipping, and controlling of a military force" (citing Gilligan v. Morgan, 413 U.S. 1, 10 (1973))).

20. *See* Riley v. California, 134 S. Ct. 2473 (2014) (holding that warrantless digital search of suspect's cell phone was not covered by search incident to arrest doctrine); United States v. Jones, 132 S. Ct. 945 (2012) (limiting warrantless GPS tracking); *cf.* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 487–90 (2011) (outlining the model of courts' responses to technological change).

"About" collection under section 702 does not require the same interpretive leap as authorizing bulk metadata collection under section 215, since it hinges on the definition of the statutory term "target," which can readily encompass the collection of communications about a particular subject. Critics argue that each reading took interpretive liberties. However, their narrow reading of each statute is not the only account worthy of consideration.

Critics often pay insufficient heed to the fiduciary dimensions of secrecy and information collection. When an entity such as a labor union or the federal government invites the trust of its members or constituents,[21] the entity takes on corresponding obligations. For example, labor unions must fairly represent their members.[22] Federal officials must, within the bounds of the Constitution, provide for the safety and defense of U.S. persons from foreign and domestic threats.[23] As precedents from U.S. law and history demonstrate,[24] secrecy has often been a vital asset in meeting those obligations. While a fiduciary must often keep information secret, she must also acquire information[25] about threats to her stakeholders.[26] To that end, the Supreme Court has held that a union can obtain information that is "of use to the union in carrying out its statutory duties and responsibilities."[27]

Both bulk collection of metadata under section 215 and foreign content collection under section 702 served this fiduciary goal. While the metadata program's benefits were more diffuse, it allowed the government to quickly and reliably map out the contacts of known terrorist entities and operatives.[28] That capability generated investigative leads, even granting critics' contention that the program did not by itself foil a specific attack.[29] Moreover, the program played a useful role in allocating government resources. In chaotic situations, such as the aftermath of the Boston Marathon bombing, the program enabled investigators to discern early on that the Tsarnaev brothers acted without foreign assistance, freeing officials to concentrate on the domestic

---

21. *See* Ethan J. Leib et al., *A Fiduciary Theory of Judging*, 101 CALIF. L. REV. 699, 705–13 (2013) (discussing attributes of fiduciaries).

22. *See* Vaca v. Snipes, 386 U.S. 171, 190 (1967).

23. *See In re* Neagle, 135 U.S. 1, 59 (1890).

24. *See* Tenet v. Doe, 544 U.S. 1, 11 (2005).

25. *See* NLRB v. Acme Indus. Co., 385 U.S. 432, 437 (1967).

26. *Cf.* Peter Margulies, *Advising Terrorism: Material Support, Safe Harbors, and Freedom of Speech*, 63 HASTINGS L.J. 455, 473–75 (2012) (discussing Founding Era views of risks posed by asymmetries in information between nations).

27. *Acme*, 385 U.S. at 437.

28. ACLU v. Clapper, 959 F. Supp. 2d 724, 746 (S.D.N.Y. 2013).

29. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, 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 150 (Jan. 23, 2014) [hereinafter PCLOB SECTION 215 REPORT].

realm.[30] Even critics of the metadata program have agreed that section 702 has assisted the government in obtaining information "efficiently and effectively about foreign targets overseas."[31]

A fiduciary's power to obtain information is subject to vital restraints. The executive branch typically must act within a framework created by its co-equal political branch, Congress.[32] Such constraints also shape the metadata program. In section 215, Congress required that the executive request information through the FISC, which authorized queries of metadata only with a small set of call numbers for which the agency had a "reasonable, articulable suspicion" of links to terrorism.[33] This particularized search protocol matched approaches that courts have required in the approval of warrants to search digital information.[34] In addition, the Department of Justice had to provide regular updates to both the intelligence and judiciary committees of the Senate and House of Representatives.[35] While not all members of Congress availed themselves of the information the government proffered, the information was sufficient to fuel eloquent critiques of the program from engaged legislators.[36]

As with any safeguards, such protections prove themselves not in text or theory but in the situation "on the ground." From the metadata program's inception in mid-2006 to early 2009, the NSA did not comply with the particularized search constraints imposed by the FISC. However, once the Justice Department learned of this serious compliance issue and alerted the FISC, the court imposed a rigorous remedial regime that brought the NSA into compliance.[37] That compliance regime included automated controls on NSA searches and regular reporting to the FISC. Government disclosures to Congress were

---

30. *See* PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 104 (DEC. 12, 2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

31. *Id.* at 144; *cf.* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 93 (July 2, 2014) [hereinafter PCLOB SECTION 702 REPORT].

32. *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring); Samuel Issacharoff & Richard H. Pildes, *Between Civil Libertarianism and Executive Unilateralism: An Institutional Process Approach to Rights During Wartime, in* THE CONSTITUTION IN WARTIME: BEYOND ALARMISM AND COMPLACENCY 171, 173–76 (Mark Tushnet ed., 2005) (arguing that courts defer more to executive decisions on national security when the President acts with Congress's support).

33. *See In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Name Redacted by Court], No. BR 06-05, 2006 WL 7137486, at *2 (FISA Ct. May 24, 2006).

34. *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010) (en banc).

35. 50 U.S.C. § 1871(a)(4)–(5) (2014).

36. *See* Lizza, *supra* note 10, at 59.

37. *See In re* Prod. of Tangible Things from [Name Redacted by Court], No. BR 08-13, 2009 WL 9150913, at *5-10 (FISA Ct. Mar. 2, 2009).

adequate, although the written disclosures exhibited an unhelpful tendency to blame mistakes on machines, not people.[38]

Now that Snowden's revelations have mooted some of the secrecy surrounding both section 215 and section 702, the dynamic conception encompasses reforms that stress tailoring of surveillance and the optimal balance of external and internal constraints. Those constraints should include a robust public advocate at the FISC. That public advocate could help ensure that the NSA faithfully implements any congressional changes to the section 215 program, such as requirements that would keep call records with phone carriers and permit the government to ask the FISC to order the carriers to produce information based on a "specific selection term."[39] A public advocate could also ensure that "about" collection under section 702 can remain tailored, and can ensure more specific criteria for U.S. person queries of section 702 data.

A July 2014 compromise reform package negotiated by Senator Patrick Leahy of Vermont and executive branch representatives[40] includes significant improvements to tailoring and external constraints, although it fails to embrace an institutionalized public advocate. The USA Freedom Act introduced by Senator Leahy (the "Leahy bill"), which is likely to be the template for legislation enacted by Congress, tightens requirements for government requests for metadata and authorizes the FISC to appoint amici curiae to advocate for privacy and civil liberties. It also permits the FISC to certify legal questions to the Foreign Intelligence Surveillance Court of Review ("FISCR"), and in turn, authorizes the FISCR to certify legal questions to the U.S. Supreme Court. It is not clear, however, that the changes wrought by the Leahy bill, if enacted into law, will produce the desired results.

This Article argues that, as is perhaps inevitable in a compromise, the Leahy bill makes progress toward reform but will produce less positive change than its drafters hoped. The definition of the "specific selection term" that the government must cite to gain access to metadata may prompt unduly narrow judicial interpretations. I argue that courts should read the definition to permit access to data that the government can currently request through ordinary means, such as grand jury subpoenas. In contrast to the tightening of section 215, the Leahy bill

---

38. *See* RONALD WEICH, REPORT ON THE NSA'S BULK COLLECTION PROGRAMS AFFECTED BY USA PATRIOT ACT REAUTHORIZATION 4 (Dec. 14, 2009), *available at* http://www.emptywheel.net/wp-content/uploads/2013/08/091214-FISA-Cover-Letter-to-Reyes.pdf.

39. *See* USA FREEDOM Act, H.R. 3361, 113th Cong. § 101(a)(3) (as passed by H.R., May 22, 2014).

40. *See* USA FREEDOM Act of 2014, S. 2685, 113th Cong. (introduced July 30, 2014), entitled "A bill introduced by Senator Patrick Leahy, et al., to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes."

makes no substantive changes to the section 702 program to further limit NSA analysts' access to U.S. person data, although some changes would enhance the long-term legitimacy of section 702. The Leahy bill's institutional reforms, while salutary in a number of respects, do not go far enough. The amicus curiae approach hinges on FISC appointment of amici, which may flounder because of the FISC's skepticism about an adversarial process. Certification, which has fallen into disuse at the Supreme Court, may also fail to provide the effective resolution of legal issues that reformers desire.

One brake on more far-reaching institutional reform has been concern that changes could trigger problems under Article III's "case and controversy" requirement and the Appointments Clause in Article II. In particular, some have worried that a robust public advocate would press for a discussion of broad legal or policy matters, without the individualized stake that is required by Article III, and that the appointment of a public advocate by the courts would raise Appointments Clause issues.[41] A dynamic conception would reject those formalistic arguments. This Article argues that the Supreme Court's decision in *United States v. United States District Court (Keith)*,[42] which invited action by Congress that eventually led to FISA, gives Congress substantial latitude in fashioning institutional reforms.

In *Keith* and in *Morrison v. Olson*,[43] which upheld Congress's enactment of the independent counsel statute after the crisis of confidence brought on by Watergate, the Court eschewed formalism and deferred to efforts by Congress to remedy perceived failures of deliberation. That approach mirrors the historic place of *ex parte* warrant applications under Article III. As the Justice Department's Office of Legal Counsel told Congress before it enacted FISA, the manifest need for independent review of warrant applications has always trumped a formalistic reading of Article III exercise of judicial power. The Court would approach new reforms to the FISA process in the same manner, as measures designed to enhance the independence of the judiciary and signal the legitimacy of surveillance efforts.

This Article is divided into five parts. Part I outlines the operation of the metadata program and section 702. Parts II–IV address the metadata program. Part II analyzes ambiguity in section 215's text. Part III argues that the fiduciary conception of relevance is a reasonable interpretation of the statute, especially in light of the history of

41. *See* ANDREW NOLAN ET AL., CONG. RESEARCH SERV., R43260, REFORM OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS: INTRODUCING A PUBLIC ADVOCATE (Mar. 21, 2014); Orin Kerr, *Article III Problems with Appellate Review in the Leahy Bill?*, LAWFARE (July 30, 2014), http://www.lawfareblog.com/2014/07/article-iii-problems-with-appellate-review-in-the-leahy-bill/.

42. 407 U.S. 297, 306–08 (1972).

43. 487 U.S. 654 (1988).

government secrecy and technology in national security matters. Part IV considers the metadata program's pre-Snowden operation, noting its "trial by fire" in 2009 when the government disclosed the NSA's noncompliance with the FISC's conditions. Part V discusses the post-Snowden landscape, suggesting that tailoring and external constraints shape the analysis of the Leahy bill and other proposed changes to section 215 and section 702.

I. The Statutory Framework

Our inquiry starts with the statutory provisions at issue: section 215 of the USA Patriot Act and section 702 of FISA. This Part discusses the statutes' text, the relevant case law, and the operation of the activities that courts have authorized under each provision.

A. Section 215

1. Text and Case Law

Section 215 of the USA Patriot Act, as amended in 2006, allows the government to obtain, with court approval, records, and tangible things that are "relevant to an authorized investigation . . . to protect against international terrorism."[44] The "relevance standard" revised language from the original Patriot Act of 2001, passed shortly after the September 11 attacks, which, with court approval, permitted the government to obtain tangible things "sought . . . in an investigation." Congress added the relevance standard for clarity, but legislative history indicates that by making this change, Congress did not wish to alter the government's access to information.[45]

All government applications under section 215 go to the FISC, a court comprised of a rotating group of Article III judges appointed by the Chief Justice of the U.S. Supreme Court. Most of the FISC's docket involves applications that the government makes *ex parte*, just as warrant applications by state, local, and federal law enforcement officials have been made for over two centuries.[46] Often, the government makes a

44. 50 U.S.C. § 1861(b)(2)(A) (2006). The statute lists "presumptively relevant" items including those pertaining to a foreign power or "agent of a foreign power," the "activities" of said agent, or "an individual in contact with, or known to, a suspected agent of a foreign power." *Id.* § 1861(b)(2)(A)(i)–(iii). In addition, the NSA collects the content of communications in which at least one party is a non-U.S. person reasonably believed to be located abroad when the surveillance will result in acquiring foreign intelligence information. *See* FISA Amendments Act of 2008 § 702, 50 U.S.C. § 1881a (2014). Discussion of section 702 and human rights is beyond the scope of this Article. For analysis, see Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and Int'l Counterterrorism*, 82 Fordham L. Rev. 2137 (2014).

45. H.R. Rep. No. 109-333, at 11302 (2005) (Conf. Rep.) (noting that the change was not intended to "prevent the FBI from obtaining tangible items that it can currently obtain").

46. *Keith*, 407 U.S. 297, 316 (1972).

preliminary application to the FISC, which the court indicates that it will approve on condition that the government makes changes that narrow the request. Once the government makes these changes, the FISC approves the application. While some critics of the metadata program and other proceedings under FISA assert that the FISC's high approval rate makes it a "rubber stamp," this critique misses the "iterative process" that characterizes litigation in that court.[47]

The first opinion to authorize bulk collection was a 2004 opinion by Judge Kollar-Kotelly that granted the government's application under FISA to use a pen register to collect information on the routing or addressing of e-mails, excluding the content of communications.[48] This opinion introduced a concept that would shape collection in the years to come: it coupled authority for the wide *collection* of information by the government with significant restrictions on the government's *use* of that information. Judge Kollar-Kotelly assumed that a relevance standard governed both pen registers and FISC orders under section 215.[49] Finding that the statutory language in the FISA pen register provision did not require that the government identify specific targets prior to collection, Judge Kollar-Kotelly acknowledged that the statute allowed "exceptionally broad" acquisition of e-mail records,[50] most of which would be "unrelated" to terrorism.[51] To avoid giving the government the unchecked ability to rummage through these mountains of data, Judge Kollar-Kotelly added restrictions on government analysts' access to the information collected. When structuring queries of the electronic data, Judge Kollar-Kotelly held that analysts could use only those e-mail addresses specifically linked to particular terrorist organizations.[52] No other queries—for example, addresses of celebrities or government critics—were permissible.

Supporting her analysis, Judge Kollar-Kotelly suggested that Congress intended the relevance standard in the pen register provision to broaden information gathering for national security purposes. The

47. *See* ACLU v. Clapper, 959 F. Supp. 2d 724, 744 (S.D.N.Y. 2013).

48. [Case Name Redacted], No. PR/TT [redacted], at 13 (FISA Ct.), *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf [hereinafter Kollar-Kotelly Opinion]; 50 U.S.C. § 1842(c)(2) (2011) (authorizing pen register to acquire information "relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities"). While the date of the Kollar-Kotelly decision does not appear in the version released to the public, accounts uniformly set the date as July 2004. *See* Lizza, *supra* note 10, at 54 (giving the date as July 14, 2004); *cf. Case Profile*, THE CIV. RTS. LITIG. CLEARINGHOUSE, http://www.clearinghouse.net/detail.php?id=13107 (last visited Dec. 14, 2014).

49. Kollar-Kotelly Opinion, *supra* note 48, at 19. This view preceded the 2006 amendment of section 215 that formally introduced a relevance standard.

50. *Id.* at 21, 23.

51. *Id.* at 28.

52. *Id.* at 42 (citing standard of "reasonable articulable suspicion" of terrorist ties).

relevance standard replaced language that required only a "reasonable suspicion" that the communication facility subject to the pen register be used by an individual engaged in "international terrorism or clandestine intelligence activities."[53] Collecting e-mail metadata from a range of Internet service providers ("ISPs") would meet the relevance standard, the court found, accepting the government's argument.[54] Broad collection would allow the government to ferret out previously unknown e-mail addresses linked to terrorism, which "more precisely targeted forms of collection against known accounts" would exclude.[55] The court defended its deference to the government's rationale, finding that, "for reasons of both constitutional authority and practical competence, deference should be given to the fully considered judgment of the executive branch in assessing and responding to national security threats and in determining the potential significance of intelligence-related information."[56]

In 2006, in a much shorter opinion, the FISC granted the government's request under section 215 to authorize the bulk collection of metadata on virtually all land-line telephone calls originating in or received in the United States.[57] Like Judge Kollar-Kotelly's opinion, this opinion conditioned wide collection authority for the government on observance of substantial restrictions on access to the data collected.[58] The court allowed the government to acquire this huge database of phone numbers (again, not content), but sharply limited analysts' access to the metadata. Rather than run any search the analysts could think up, the FISC limited the NSA to search queries containing specific phone numbers, or "identifiers."[59] For each identifier, a senior NSA official had to have a "reasonable and articulable suspicion" ("RAS") of connections to a listed terrorist group.[60] The FISC approves the terrorist groups that appear on the list[61] and receive reports every thirty days on search

53. *Id.* at 29 n.21 (citing Pub. L. No. 105-272, § 601(2)).

54. *Id.* at 48–49.

55. *Id.* at 42 (adding that the "NSA needs bulk collection in order to identify unknown . . . communications" linked to terrorist groups).

56. *Id.* at 30 (citing Dep't of Navy v. Egan, 484 U.S. 518, 529 (1988)).

57. *See In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Name Redacted by Court], No. BR 06-05, 2006 WL 7137486, at *1 (FISA Ct. May 24, 2006).

58. *Id.* at *11.

59. David S. Kris, *On the Bulk Collection of Tangible Things*, LAWFARE RES. PAPER SERIES, Sept. 29, 2013, at 10, *available at* http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf; Steven G. Bradbury, *Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702*, LAWFARE RES. PAPER SERIES, Sept. 1, 2013, at 2–3, *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/Bradbury-Vol-1-No-3.pdf.

60. Kris, *supra* note 59, at 10–11.

61. *Id.*

results.[62] Pursuant to the FISC's 2006 order, analysts querying the database with RAS-approved identifiers could search up to three "hops" from the identifier, for example, persons called by someone using an RAS-approved identifier, persons called by the recipient of that call, and the persons called by that second group of recipients.[63] In January of 2014, after the Snowden disclosures, President Obama asked the FISC to approve in advance all identifiers used by NSA analysts. The President also limited the NSA to data it could acquire through only two hops, not the previous three.[64]

Legislation passed by the House of Representatives in May 2014 and pending in the Senate as of July 2014 went further. The House bill limited government collection, leaving metadata in the hands of private companies. It also required the government to seek court orders from the FISC requiring telecommunications companies to produce records based on a "specific selection term" related to a foreign power or agent of a foreign power and other records up to two hops removed from this term. The House defined "specific selection term" as "a discrete term, such as a term specifically identifying a person, entity, account, address, or *device*, used by the Government to limit the scope of the information or tangible things sought."[65]

2. The Uses of Metadata

The utility of the metadata program has been the subject of vigorous debate, with the government initially insisting that the program was "essential" and critics suggesting that the government's claims were inflated.[66] The fog of rhetoric on both sides obscures common ground. The program cannot claim exclusive credit for stopping a terrorist plot,[67] and in most investigations other alternatives could have provided (or actually did provide) information that identified the plotters. However, the most careful and comprehensive critics concede that the program has provided early information in investigations, allowed law enforcement to rule out suspects, and hedged against the persistent problem of disparate agencies failing to "connect the dots."[68]

---

62. *Id.* at 11. In 2012, there were fewer than 300 RAS-approved identifiers. *Id.* at 12.

63. *Id.* at 12.

64. *See* Obama, *supra* note 1.

65. H.R. 3361 113th Cong. § 107(k)(2) (as reported by the Committee on Judiciary and the Committee on Intelligence May 15, 2014), amending 50 U.S.C. § 1861 (emphasis added); *see* USA FREEDOM Act of 2014, S. 2685, 113th Cong. (introduced July 30, 2014) (narrowing definition of selection term).

66. *See* Ellen Nakashima, *Skepticism Deepens About NSA Program*, WASH. POST, Aug. 1, 2013, at A1.

67. *See* PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMC'NS TECHS., *supra* note 30, at 104 (asserting without analysis that program is "not essential to preventing attacks").

68. ACLU v. Clapper, 959 F. Supp. 2d 724, 746 (S.D.N.Y. 2013) (finding that the program allows government to perform "the algorithmic data analysis to find 'connections between known and

The single court to squarely address this question has agreed that the program is helpful because it allows the government to effectively, reliably, and expeditiously trace connections between known and unknown terrorists.[69] Having a large database enhances the comprehensiveness of the government's search for connections. As the district court noted in *ACLU v. Clapper*, "without all the data points, the Government cannot be certain it connected the pertinent ones."[70] Having a *single* large database avoids the waste of time entailed in chasing down leads with different telecommunications providers.[71] Promulgating a single set of rules for that database ensures that data will be deleted only when the government, taking both security and privacy into account, is confident that the data is irrelevant.

For an illustration of the benefits and limits of the metadata program, consider the case of Najibullah Zazi, who had plotted in 2009 to bomb New York City subways.[72] Pursuant to the metadata program, the NSA provided the Federal Bureau of Investigation ("FBI") with information "early in the investigation" showing Zazi's telephone calls.[73] The NSA also provided the FBI with "additional leads" throughout the investigation.[74] Moreover, the NSA used section 215 to ascertain the unknown telephone number of one of Zazi's New York accomplices, Adis Medunjanin.[75] While this information may well have been available from other sources,[76] the metadata program is what provided the facts.

The metadata program also plays an important role in allocating government counterterrorism resources. For example, as Ryan Goodman suggests, the comprehensive nature of the section 215 program

---

unknown international terrorist operatives'"). The court undertook this analysis despite finding that section 215's statutory scheme precluded individual suits for injunctive relief. *Id.* at 32–42.

69. *Id.*

70. *Id. Clapper* and another district court have come to opposite conclusions on whether the bulk collection of metadata constitutes a search under the Fourth Amendment. *Compare id.* at 749–52 (holding that individual caller has no reasonable expectation of privacy in telecommunications companies' call records), *with* Klayman v. Obama, 957 F. Supp. 2d 1, 25–29, 41 (D.D.C. 2013) (finding that metadata program constitutes unreasonable search); *cf.* Smith v. Maryland, 442 U.S. 735, 742–43 (1979) (articulating the "third-party doctrine," which holds that individual has no reasonable expectation of privacy in items such as call records that are voluntarily shared with a third party in the course of creating such records). *But see* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK 156–58 (2007) (critiquing third-party doctrine). I refer to this issue later in the piece. *See infra* note 262 and accompanying text (noting debate about whether government access to "mosaic" of metadata showing individuals' habits and beliefs triggers expectation of privacy). However, definitive analysis of the Fourth Amendment issue is beyond the scope of this Article.

71. *See* PCLOB SECTION 702 REPORT, *supra* note 31, at 155 n.556 (conceding that telecommunications companies "likely vary" in their speed in responding to government requests).

72. *Id.* at 149–52.

73. *Id.* at 150.

74. *Id.*

75. *Id.*

76. *Id.*

allows the government to rule out foreign connections to plots, such as the Boston Marathon bombing.[77] While this capability may not be as eye-catching as the ability to ferret out a pending plot, it can help law enforcement and national security officials allocate resources in the long and short term. In the long term, the metadata program gives officials a view from 20,000 feet on the links to international terrorist groups within the United States. If queries show a relatively small presence, officials can focus their efforts narrowly, and devote more resources to foreign threats. The metadata program reduces the guesswork involved in allocation decisions, and solidifies the factual foundation for these complex determinations. In the near term, the metadata program can inform allocation of resources in the chaotic period immediately following an attack. During the Boston Marathon bombing investigation, for example, section 215 collection helped to confirm early on that the Tsarnaev brothers acted without foreign assistance.[78] That confirmation curbed counterproductive speculation, and focused resources on the Tsarnaev brothers' roles.[79]

The metadata program also provides for efficiency in tracing contacts. In some investigations, speed may turn out to be less important because law enforcement officials are gathering information and monitoring a subject over time. However, as Director of the FBI James Comey testified to Congress in January 2014, the "agility" produced by the metadata program may turn out to be quite useful in a fast-moving investigation. Comey put it simply: that agility, which permits law enforcement to accomplish "in minutes what would otherwise take . . . hours," is "not material except when it matters most."[80]

Finally, the metadata program is a useful hedge if agencies fail to share information that could allow them to connect the dots in a counterterrorism investigation. This failure was the most salient problem with the actions of law enforcement and security officials prior to the September 11 attacks.[81] Although the situation has improved,[82] deficits in cooperation will inevitably occur whenever agencies seek to coexist.[83]

---

77. *See* Ryan Goodman, *How to Evaluate Whether the NSA's Telephony Metadata Program Makes Us Safer (and What Proponents and Opponents Get Wrong)*, JUST SECURITY (Dec. 27, 2013, 9:13 AM), http://justsecurity.org/2013/12/27/effectiveness-telephony-metadata-program/; *cf.* PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMC'NS TECHS., *supra* note 30, at 104 (acknowledging that "negative results from section 215 queries have helped to alleviate concern that particular terrorist suspects are in contact with co-conspirators in the United States," while asserting that the metadata program is too small to provide comprehensive information on this point).

78. Goodman, *supra* note 77.

79. *Id.*

80. Senate Select Intelligence Comm., *Current and Projected National Security Threats Against the U.S.*, FED. NEWS SERV., Jan. 29, 2014.

81. PCLOB SECTION 702 REPORT, *supra* note 31, at 153–55.

B. Section 702

Under section 702 of the FISA Amendments Act of 2008 ("FAA"),[84] the government may conduct surveillance targeting the contents of communications of non-U.S. persons reasonably believed to be located abroad when the surveillance will result in acquiring foreign intelligence information.[85] Pursuant to the FAA, the government must file a certification with the FISC that details its targeting procedures, as well as minimization procedures that reduce the likelihood that analysts will use or retain purely domestic communications or irrelevant information about U.S. persons, defined as U.S. citizens and lawful permanent residents.[86] The FISC can review these and other materials to determine whether the government has complied with the statute, although the FISC does not need to approve individual targets selected by the government.[87]

Under section 702, foreign intelligence information that the government may acquire includes data related to national security, such as information concerning an "actual or potential attack" or "other grave hostile acts [by a] foreign power or an agent of a foreign power."[88] Foreign intelligence information also comprises information relating to possible sabotage[89] and clandestine foreign "intelligence activities."[90] Another prong of the definition is broader, encompassing information relating to the "the conduct of the foreign affairs of the United States."[91]

The absence of a requirement for FISC approval of individual targeting choices under section 702 is rooted in the constitutional status of foreign surveillance and the path to enactment of section 702. The Supreme Court held in *United States v. Verdugo-Urquidez* that non-U.S.

---

82. *See* Matthew C. Waxman, *Police and Nat'l Sec.: American Local Law Enforcement and Counterterrorism After 9/11*, 3 J. Nat'l Sec. L. & Pol'y 377, 385 (2009).

83. *See* Michael P. Robotti, *Grasping the Pendulum: Coordination Between Law Enforcement and Intelligence Officers Within the Dep't of Justice in a Post-"Wall" Era*, 64 N.Y.U. Ann. Surv. Am. L. 751, 809–19 (2009).

84. 50 U.S.C. § 1881a (2011).

85. *Id.* § 1881a(a). Portions of the discussion in this Subpart originated in an earlier piece. *See* Margulies, *supra* note 44, at 2140–41.

86. 50 U.S.C. § 1881a(c)(1)(A)–(B); *id.* § 1801(i).

87. *See* President's Review Group on Intelligence and Commc'ns Techs., *supra* note 30, at 135. The Attorney General and Director of National Intelligence can issue a determination that permits surveillance without prior FISC approval when exigent circumstances so require. Exigent circumstances exist when, without immediate action, "intelligence important to the national security of the United States may be lost or not timely acquired." 50 U.S.C. § 1881(c)(2). In this exigent situation, the Attorney General and Director of National Intelligence must submit a certification to the FISC seeking authorization within seven days. *Id.* § 1881(g)(1)(B).

88. *Id.* § 1801(e)(1)(A).

89. *Id.* § 1801(e)(1)(B).

90. *Id.* § 1801(e)(1)(C).

91. *Id.* § 1801(e)(2)(B).

persons (defined as those other than U.S. citizens, lawful permanent residents, or located in the territorial United States) do not enjoy the protections of the Fourth Amendment.[92] Chief Justice Rehnquist, writing for the Court, explained that the Fourth Amendment uses the term "*the* people" to identify beneficiaries of the amendment's "right . . . to be secure in . . . persons, houses, papers, and effects, against unreasonable searches and seizures."[93] The phrase "the people," according to the Chief Justice, was a "term of art" that occurs elsewhere in the Constitution and in each case refers to the "people of the United States."[94]

Moreover, functional considerations weigh against subjecting foreign searches and seizures to the restrictions imposed by the Fourth Amendment, including the requirement of an individualized warrant. Subjects of surveillance abroad might be harbored by foreign states that are indifferent or even hostile to U.S. law enforcement, and U.S. courts might not have authority over foreign courts, making the issuance of a warrant a futile exercise. Consequently, the Supreme Court has generally interpreted rights against search and seizure under the Fourth Amendment to include only U.S. citizens, legal permanent residents, or those physically present in the United States.[95]

Even with respect to searches and seizures abroad concerning U.S. citizens or lawful permanent residents, courts have held that there is a "foreign intelligence exception" to the warrant requirement of the Fourth Amendment. In *United States v. Truong Dinh Hung*, a case involving a Vietnamese national in the United States who had sought to convey sensitive U.S. diplomatic cables to Vietnamese negotiators, the Fourth Circuit located the rationale for such an exception in the need for "stealth, speed, and secrecy" in countering foreign threats, and in the executive's expertise and constitutional responsibility in the area of foreign affairs.[96]

In *Keith*, the Supreme Court, while not completely resolving this issue, invited Congress to legislate on the requirements for national security searches.[97] In response to this invitation and executive abuses involving warrantless surveillance of U.S. citizens within the United States that the Court had addressed in *Keith*, Congress enacted FISA, which imposed requirements on the executive for conducting

92. 494 U.S. 259, 265 (1990).

93. *Id.*; U.S. CONST. amend. IV (emphasis added).

94. *Verdugo-Urquidez*, 494 U.S. at 265.

95. *Id.* at 274–75.

96. 629 F.2d 908, 913 (4th Cir. 1980); *see In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008) (discussing foreign intelligence exception for warrant requirement); United States v. Duka, 671 F.3d 329, 341 (3rd Cir. 2011) (same); United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *18 (D. Ore. June 24, 2014) (same).

97. *Keith*, 407 U.S. 297, 322 (1972).

surveillance in the United States on an agent of a foreign power. Those requirements included an individualized warrant.

The George W. Bush administration, in the aftermath of the 9/11 attacks, decided, based on a questionable legal opinion from the Justice Department, that it could disregard FISA.[98] It unilaterally initiated a sweeping surveillance initiative known as the Terrorist Surveillance Program ("TSP"), based on the President's Article II authority, or on implied authority derived from the Authorization for the Use of Military Force that Congress had enacted for the U.S. intervention in Afghanistan after September 11.[99] After the TSP came to light in late 2005, the administration sought and received authorization from the FISC for portions of the program.[100] Shifts in the FISC's position on the legality of the program led to passage of the Protect America Act ("PAA").[101] Congress worried, however, that the PAA did not provide sufficient protections for U.S. persons. In 2008, Congress, including then-Senator Barack Obama, enacted the FAA on a bipartisan vote.[102]

According to the President's Review Group, which President Barack Obama commissioned to study surveillance after the Snowden disclosures, section 702 has played a concrete role in keeping the nation safe.[103] The Review Group's report asserted that section 702 was "critical" to the uncovering of the Zazi planned subway attack in New York in 2009, and led to the arrest of Zazi and his accomplices.[104] The section 702 program resulted in obtaining information that "contributed in some degree" to a successful outcome regarding thwarted terrorist attacks in the United States and other countries in fifty-three out of fifty-four instances.[105] According to the Review Group, section 702 "does in fact play an important role in the nation's effort to prevent terrorist attacks across the globe."[106] The Privacy and Civil Liberties Oversight Board ("PCLOB") agreed with this assessment, concluding that collection under section 702 "significantly aids the government's efforts

98. *See* OFFICE OF THE INSPECTOR GEN. OF THE DEP'T OF DEF. ET AL., UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 10–13 (2009), *available at* http://fas.org/irp/eprint/psp.pdf.

99. DEP'T OF JUSTICE, THE NSA PROGRAM TO DETECT AND PREVENT TERRORIST ATTACKS: MYTH V. REALITY 1 (2006), *available at* http://www.justice.gov/sites/default/files/opa/legacy/2006/02/02/nsa_myth_v_reality.pdf.

100. Letter from Alberto Gonzales, Att'y Gen. of the U.S., to Senators Patrick Leahy & Arlen Specter (Jan. 17, 2007), *available at* http://graphics8.nytimes.com/packages/pdf/politics/20060117gonzales_Letter.pdf; *cf.* Clark, *supra* note 231, at 403 (discussing chronology of events).

101. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007) (codified as amended in various sections of 50 U.S.C.)

102. 154 CONG. REC. S6470 (daily ed. July 9, 2008).

103. *See* PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMC'NS TECHS., *supra* note 30, at 143.

104. *Id.* at 143–44.

105. *Id.* at 144–45.

106. *Id.* at 145.

to prevent terrorism . . . combat weapons proliferation and gather foreign intelligence."[107]

II. Relevance Under Section 215: Statutory Ambiguity and *Chevron*

Because the FISC's approval of the metadata program has its roots in Judge Kollar-Kotelly's 2004 Internet pen register opinion, it is useful to analyze the statutory issue of relevance under section 215 as Judge Kollar-Kotelly did under the pen register statute: as a matter of deference to executive interpretation. Judge Kollar-Kotelly deferred to the executive branch, just as the Supreme Court has done in many other cases pertaining to national security, such as *Department of Navy v. Egan*.[108] In a statutory context, two steps sum up the government's claim that deference is owed. First, a court asks whether the statute is ambiguous.[109] If that court finds that the statute is ambiguous, the court moves on to step two, and asks whether the government's interpretation is reasonable.[110] This Part addresses the first step.

A. Defining Relevance Down: A Tale of Three Dictionaries

Two definitional questions flow from the phrase "relevant to an authorized investigation"[111] in the pre-Snowden version of section 215.[112] The first is the meaning of relevance. The second is the meaning of "an authorized investigation." Critics of the metadata program do not regard this language as ambiguous. Instead, they assert that relevance under section 215 is clear, requiring a substantive link to investigation of a particular crime.[113] In contrast, the FISC and at least one federal district

107. *See* PCLOB Section 702 Report, *supra* note 31, at 93.

108. 484 U.S. 518, 530 (1988). For the central Supreme Court case on deference to administrative agencies, see Chevron, U.S.A., Inc. v. Natural Res. Def. Council, 467 U.S. 837, 863 (1984); *cf.* Curtis A. Bradley, Chevron *Deference and Foreign Affairs*, 86 Va. L. Rev. 649, 668–75 (2000) (discussing virtues of appropriately cabined doctrine of deference in foreign affairs); Eric A. Posner & Cass R. Sunstein, Chevron*izing Foreign Relations Law*, 116 Yale L.J. 1170 (2007) (arguing for deference to the executive); Derek Jinks & Neal Kumar Katyal, *Disregarding Foreign Relations Law*, 116 Yale L.J. 1230, 1257–75 (2007) (arguing against blanket deference to the executive); *cf.* Cass R. Sunstein, *Admin. Law Goes to War*, 118 Harv. L. Rev. 2663, 2669–70 (2005) (arguing that deference to presidential interpretations can be problematic when deference conflicts with civil liberties); Joseph Landau, Chevron *Meets* Youngstown*: Nat'l Sec. and the Admin. State*, 92 B.U.L. Rev. 1917, 1924–25 (2012) (discussing *Chevron* deference and the separation of powers in national security cases).

109. *Chevron*, 467 U.S. at 842–43.

110. *Id.* at 843.

111. 50 U.S.C. § 1861(b)(2)(A) (2006).

112. I use the phrase "pre-Snowden" to refer to the version of section 215 that was in effect at the time of Snowden's revelations. That version was still in effect as of July, 2014, although the House bill passed in May 2014 heralded substantial changes that will emerge in final form when the Senate takes up the bill later in 2014.

113. *See* Donohue, *supra* note 8 (manuscript at 58).

court have viewed the statutory language more broadly,[114] suggesting that relevance can entail a relationship to the function of the investigating agency. Moreover, an investigation need not focus on a particular crime; it can instead be a wide-ranging inquiry into a category of wrongdoing, such as international terrorism.[115]

Dictionaries do not resolve the debate. According to the Supreme Court, "Congress intends to incorporate the well-settled meaning of the . . . terms it uses."[116] With relevance, however, well-settled meanings seem built on semantic sand. Merriam-Webster's Dictionary defines the term "relevant" as "having significant and demonstrable bearing on the matter at hand."[117] Secondary definitions include the following: "affording evidence tending to prove or disprove the matter at issue or under discussion" or being "proportional" or "relative" to a particular item.[118] The Oxford English Dictionary is even less illuminating; it defines "relevant" as "legally pertinent or sufficient," adding as a secondary meaning, "[b]earing on, connected with, or pertinent to the matter at hand."[119] Black's Law Dictionary is hardly more enlightening. It defines "relevant" as "[a]pplying to the matter in question; affording something to the purpose."[120] What that special "something" is, however, remains unclear. In sum, the dictionary definitions of relevance only heighten the ambiguity of the statute's text.

B. Metadata's Critics on Case Law and Legislative History

Critics have made headway when they turn to case law.[121] Even though the decisions regularly extol the relevance standard's flexibility,[122] case law typically deals with investigations of wrongdoing by a specific individual, group, or entity. For example, in *United States v. Arthur Young & Co.*, the Supreme Court upheld a request by the Internal Revenue Service ("IRS") for documents and other information related to the accuracy of a corporation's tax return.[123] In construing the definition of relevance under a provision of the Internal Revenue Code

114. *Id.*

115. Kris, *supra* note 59, at 18–20.

116. Neder v. United States, 527 U.S. 1, 23 (1999).

117. *See* Merriam-Webster's Collegiate Dictionary 1051 (11th ed. 2003).

118. *Id.*

119. The Oxford English Dictionary 561 (2d ed. 1989).

120. Black's Law Dictionary 1455 (4th ed. 1968).

121. For an excellent survey, see PCLOB Section 702 Report, *supra* note 31, at 63–78 (arguing that government's definition does not fit context of cases).

122. *See* First Fin. Bank, N.A. v. Bauknecht, No. 12-CV-1509, 2013 WL 3833039, at * 1 (C.D. Ill. July 23, 2013) (noting that "the discovery relevance standard is flexible"); *In re* H&R Block Mortg. Corp., No. 2:06-MD-230 (MDL 1767), 2007 WL 325351, at *2 (N.D. Ind. Jan. 30, 2007) (citing Fed. R. Civ. P. 26(b)(1) advisory committee's note that in discovery, "a flexible treatment of relevance is required.").

123. 465 U.S. 805, 814 (1984).

governing IRS inquiries, the Court stressed the importance of flexibility, even requiring production of documents that the corporation had not used to prepare its return if those documents could provide information on the corporation's overall tendency to take aggressive positions on taxes owed.[124] Courts reviewing grand jury subpoenas will sometimes assess relevance with respect to entire categories of documents, which may include vast numbers of individual items.[125] Nevertheless, as a balanced assessment of section 215 acknowledges, the investigations at issue in the cases were relatively discrete, compared to the comprehensiveness of bulk collection in the metadata program.[126] Based on the case law, critics can plausibly argue that relevance under section 215 should concern specific investigations, not the collection of a substantial percentage of U.S. call records.

The legislative history of section 215's amendment in 2006 also provides some support for the critics' view, although a significant strand in that history bolsters a broader conception. Supporters of a narrow view, which ties relevance to discrete investigations, can point to statements from Republican Senator Jon Kyl of Arizona, who described relevance as:

> "a term that every court uses . . . in every other situation in the country . . . the standard employed for the issuance of discovery orders in civil litigation, grand jury subpoenas in a criminal investigation, and for each and every one of the 335 different administrative subpoenas currently authorized by the United States Code."[127]

Senator Orrin Hatch also seemed to accept such limits, reminding his colleagues that "no section 215 order can be issued for material that would be beyond the scope of a grand jury subpoena."[128]

C. A Contrasting View: Relevance and the Government's Role

While the narrow account of relevance finds some support in the case law and legislative history, an alternative reading is also possible. This reading anchors relevance in the relationship between the information requested and the requester's role. A requesting entity's role

---

124. *Id.* at 814–15.

125. *See In re* Grand Jury Proceedings, 616 F.3d 1186, 1202 (10th Cir. 2010).

126. *See* Kris, *supra* note 59, at 23 n.84.

127. *See* 152 Cong. Rec. S1395 (daily ed. Feb. 16, 2006) (statement of Sen. Kyl). While on its face this statement suggests that Congress regarded bulk collection as a piece of more targeted information gathering, Kyl nowhere mentions metadata expressly. Kyl does mention what we know now as the section 702 program, which he describes as "surveillance . . . involving international communications with members of al-Qaida or people suspected of being with al-Qaida." *Id.* He notes the secret nature of this program, which he observes was the subject of a government briefing for "select members of the [Senate] Intelligence Committee." *Id.*

128. 51 Cong. Rec. S13,643 (daily ed. Dec. 15, 2005) (statement of Sen. Hatch).

may include fiduciary responsibilities, in which the entity functions as a repository for the trust of its members or constituents.[129]

To comply with its fiduciary obligations, the fiduciary requires information about threats and opportunities. The need for information is even more compelling when both threats and opportunities shift rapidly. The ability to adjust to that dynamic environment is a hallmark of a fiduciary's success. In managing that adjustment, a fiduciary may also be bound by limits on her authority in custom, law, or contract.[130]

A sovereign state like the United States has broad fiduciary obligations. Alexander Hamilton, writing in *The Federalist No. 23*, spoke the language of fiduciary relationships when he asserted that the "government ought to be clothed with all the powers requisite to complete execution of its trust."[131] Hamilton alluded repeatedly to this characterization, urging that the federal government receive "the most ample authority for fulfilling the objects committed to its charge,"[132] acknowledging "the responsibility [of the federal government] implied in the duty assigned to it,"[133] and describing the federal government as "that body to which the guardianship of the public safety is confided."[134] Commenting on the dynamic nature of threats and the corresponding adjustments demanded of officials discharging their responsibilities, Hamilton observed that, "it is impossible to foresee or to define the extent and variety of national exigencies, and the corresponding extent and variety of the means which may be necessary to satisfy them."[135] Yet the Framers also recognized that the government official as fiduciary faced temptations to parade out national security threats as a pretext for restraints on freedom. To guard against this danger, James Madison advised, "[a] wise nation" will not "rashly preclude itself from any resource . . . essential to its safety," but will also minimize "both the necessity and the danger of resorting to [any means] . . . which may be inauspicious to its liberties."[136]

Decisions on the scope of subpoenas or other requests for information often use language addressed not only to the substantive connection between the information sought and a particular substantive investigation, but also to the underlying function of the investigative agency or entity. In an early case on the authority of regulatory agencies, the Supreme Court held that the Interstate Commerce Commission had

---

129. *See* Leib, et al., *supra* note 21, at 705–06.
130. *Id.*
131. *See* THE FEDERALIST NO. 23, *supra* note 12, at 153–54 (Alexander Hamilton).
132. *Id.* at 155.
133. *Id.*
134. *Id.*
135. *Id.* at 153 (emphasis omitted).
136. *See* THE FEDERALIST NO. 41, *supra* note 12, at 257–58 (James Madison).

wide authority to investigate efforts to suppress competition by railroads, even without specific allegations of wrongdoing.[137] That wide authority, the Court explained, was essential to the "vigilant function" of the agency.[138] Explaining further, the Court maintained that the Commission's ambit of investigative authority "must be as comprehensive as the interest of the whole country . . . [i]f the problems which are presented to it . . . are complex and difficult," such that the definition of relevance required sufficient flexibility to meet the challenge.[139] In *Oklahoma Press Publishing Co. v. Walling*, the Court noted that the Wage and Hour Division of the Department of Labor had an "investigative function" necessary to "securing enforcement" of the Fair Labor Standards Act.[140] Harmonizing the needs of the agency and the interests of the parties from whom information is sought "cannot be reduced to formula," the Court cautioned, since "relevancy and adequacy or excess in the breadth of the subpoena are matters variable in relation to the nature, purposes, and scope of the inquiry."[141]

Modern cases echo this theme. While *Arthur Young* supports the critics' insistence on the need for a discrete investigation, it also supplies grist for the government's mill.[142] In *Arthur Young*, the Court upheld a broad subpoena of tax-related documents by the IRS, asserting that requests for documents were a "tool of discovery . . . critical to the investigative and enforcement functions of the IRS."[143] Another long chain of precedent stresses that the broad ability to request information permits labor unions to protect the interests of their members. In *NLRB v. Acme Industries. Co.*, the Court held that to investigate concerns that an employer was outsourcing labor in violation of a collective bargaining agreement, a union had to show merely that the "desired information . . . would be of use to the union in carrying out its statutory duties and responsibilities."[144]

The legislative history of section 215's enactment also supports this conception of relevance as evolving with the government's fiduciary responsibilities. For example, Senator Kyl warned that a narrow standard would make it "unnecessarily difficult for our intelligence agents and our law enforcement officers to do the job we have asked them to do."[145] Kyl

137. Smith v. Interstate Commerce Comm'n, 245 U.S. 33, 43 (1917).
138. *Id.* at 44.
139. *Id.* at 45.
140. 327 U.S. 186, 216 (1946).
141. *Id.* at 209.
142. 465 U.S. 805 (1984).
143. *Id.* at 814.
144. 385 U.S. 432, 437 (1967).
145. 152 CONG. REC. S1396 (daily ed. Feb. 16, 2006) (statement of Sen. Kyl). Senator Sessions echoed this theme, asserting that amendments requiring that the government show "specific and articulable facts" demonstrating relevance to terrorism were "unworkable and burdensome. . . [and]

emphasized that threats were dynamic, and the government's capabilities had to evolve, as well. As Kyl put it, terrorist groups are "sophisticated and devote enormous time and energy to understanding how we operate, all in service of allowing their agents to evade our investigations."[146] Responding to the threat requires "speed and . . . agility."[147] Particularly in the case of international terrorism, investigations are likely to be both broad and far ranging.[148]

Moreover, although the legislative debates on section 215 do not include discussion of intelligence gathering that mirrors the metadata program's size and scope, legislators acknowledged that the statute could authorize bulk collection. For example, Senator Carl Levin of Michigan warned that the Conference Report's language, which eventually became law, authorized information gathering of extraordinary breadth. Illustrating his concerns, Senator Levin cautioned that the FBI could look for one suspected terrorist by reviewing "all the computer user records held by public libraries in New York."[149] Moreover, Senator Levin predicted that the bill would allow the government to obtain the records of an HIV clinic, including "10,000 patient files."[150] Yet Senator Levin eventually voted for the bill with no changes to statutory language, as did a number of progressive Democratic senators, including then-Senator Obama.[151] The Senate Intelligence Committee Report may supply a clue to the progressives' shift: confidence that the FISC would require a "sufficient explanation" of relevance from the government[152] and "direct modification of the requested order"[153] to reflect the fiduciary balance between security and liberty.

D. Sunset Clauses and the Dynamic Conception

Another indicator that a broad relevance standard is a plausible construction of Congress's intent is the use of a sunset clause. Sunset clauses mandate that legislation expire at a date certain unless Congress renews the law. Congress viewed the inclusion of a sunset clause for section 215 as a means to gain experience on implementation of the

---

would undermine the ability for the investigators to do what we intended to authorize them to do." *Id.* at S1400 (statement of Sen. Sessions).

146. 152 Cong. Rec. S2437 (daily ed. Mar. 28, 2006) (statement of Sen. Kyl).

147. 152 Cong. Rec. S1395 (daily ed. Feb. 16, 2006) (statement of Sen. Kyl).

148. Kris, *supra* note 59, at 19.

149. 152 Cong. Rec. S2436 (daily ed. Mar. 28, 2006) (statement of Sen. Levin).

150. *Id.*

151. 152 Cong. Rec. S1401 (daily ed. Feb. 16, 2006) (statement of Sen. Obama) (supporting the Conference Report language that ultimately became law).

152. *See* U.S. Select Comm. on Intelligence, Report to Accompany S. 1266, S. Rep. No. 109-85, at 7 (2005).

153. *Id.*

law.[154] Keeping statutory authority on a relatively short temporal leash while allowing flexibility in implementation is a rational approach, particularly in an environment characterized by adaptive threats and rapidly changing technology.[155]

The legislative history of the USA Patriot Act confirms this characterization of sunset clauses as permitting greater flexibility. Legislators regarded the sunset clause in the Patriot Act as functionally equivalent to substantive constraints on government power. Illustrating this equivalence, legislators and the Bush administration treated inclusion of a sunset clause as a bargaining chip. Legislators got a sunset clause, which the Bush administration opposed, and, in return, legislators had to eliminate other constraints, such as limits on sharing grand jury information with other agencies, reporting provisions on government receipt of data from stored communications, and establishment of a new Inspector General position focusing on civil liberties.[156]

To facilitate information sharing by the executive on the law's implementation, Congress enacted reporting requirements. According to these requirements, the Attorney General must submit a range of information to the intelligence and judiciary committees of the House and Senate every six months.[157] That information must include a "summary of significant legal interpretations" advanced by the government in FISC proceedings[158] and the opinions of the FISC and its statutorily designated appellate court, the Foreign Intelligence Surveillance Court of Review.[159] By 2007, less than a year after the FISC authorized the bulk collection of telephony metadata, even Senator Ron Wyden of Oregon, the leading legislative opponent of the program, acknowledged that he received adequate information about the program's size, scope, and design.[160] Senator Wyden recalled that the government's disclosures triggered major substantive concerns on his part.[161] Wyden said he was shocked at what he termed "the gap between what people think the law is and how it's been secretly interpreted."[162]

---

154. 152 CONG. REC. S1402 (daily ed. Feb. 16, 2006) (statement of Sen. Feinstein) (expressing concern that the approved language on relevance in section 215 could promote "fishing expeditions . . . if not carefully monitored" and praising the sunset provisions as "important element of the continued vigorous oversight necessary" to keep statute within bounds).

155. For a different view that urges caution in addressing new technologies of surveillance without clear statutory authorization, see Orin S. Kerr, *A Rule of Lenity for National Security Surveillance Law*, 101 VA. L. REV. (forthcoming 2014), *available at* http://ssrn.com/abstract=2434326.

156. *See* Emily Berman, *The Paradox of Counterterrorism Sunset Provisions*, 81 FORDHAM L. REV. 1777, 1789 (2013).

157. *See* 50 U.S.C. § 1871 (2014).

158. *ID.* § 1871(a)(4).

159. *Id.* § 1871(a)(5).

160. *See* Lizza, *supra* note 10, at 55.

161. *Id.* "Holy Toledo!" was Wyden's first response. *Id.*

162. *Id.*

Wyden's consistent opposition to the legislation's enactment, based on the authority it granted to the government, suggests that he viewed the scope of the metadata program as predictable, rather than surprising.[163] The key point, however, is that because of the government's disclosures to Congress, Wyden had the ability to urge either amendment or outright repeal when the statute expired pursuant to the sunset clause. That built-in temporal constraint on the statute's operation is entirely consistent with a dynamic conception, which acknowledges that Congress might eventually come to view the statute as ineffective, injurious, or obsolete, and legislate accordingly.[164]

III. The Reasonableness of the Dynamic Conception of Surveillance Under Section 215

Having established that the statute is at least ambiguous, this Article now addresses the second step of the deference analysis: the reasonableness of the executive branch's position. The dynamic conception, as exemplified in the metadata program, raises difficult questions about the relationship between government secrecy and two core values in national security surveillance: deliberation and strategic advantage. Until Snowden's revelations, secrecy was central to the metadata program. Critics of the program, like Senator Wyden, regard secrecy as a prime enabler of what they perceive as the program's overreaching. However, a healthy wariness about secrecy and its ill effects should not obscure secrecy's benefits. This Part suggests that secrecy as understood by the Framers, secret dialogue between the branches of government, and case law addressing surveillance have benefits as well as costs. The same can be said for public disclosure. The dynamic conception is a reasonable alternative because it captures secrecy's benefits while leveraging participation of all three branches to reduce the cost of secrecy.

---

163. Wyden had voted against the section 215 amendments in 2006, while others like Senators Levin, Biden, and Obama who had opposed the amendments initially because of concerns about the breadth of the government's authority, eventually voted for the legislation. *Id.* at 54.

164. To focus on the larger questions of statutory interpretation, this Article will not analyze in depth whether the broad reading of relevance under section 215 clashes with other statutes, such as FISA's pen register provision, 50 U.S.C. § 1842 (2010). In the [Case name redacted] case, Judge Kollar-Kotelly opined that the FISA pen register provision is not more restrictive than section 215. Kollar-Kotelly Opinion, *supra* note 48, at 19–23. In passing the USA Patriot Act in 2001, Congress removed language that limited relevance in the pen register statute to information concerning individuals involved with international terrorism, foreign powers, or their agents. *See* USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 286, § 214(a) (2001), deleting subsection included in Intelligence Authorization Act for FY99, Pub. L. No. 105-272, 112 Stat. 2396, § 402(c)(3) (1998). This suggests that the two statutes were moving in tandem. *But see* PCLOB Section 215 Report, *supra* note 29, at 86–87 (arguing that statutes clash).

A. Deliberation and Secrecy

For a fiduciary seeking to gather information in a fluid threat environment, deliberation is vital. Deliberation entails, as Hannah Arendt suggested, the ability to look at issues from all possible angles.[165] That capacity will suggest previously unconsidered options, and may take other options off the table. In a constitutional republic, deliberation must serve a double purpose: as Hamilton explained, it must allow decisionmakers, to the extent possible, to foresee "national exigencies, and the corresponding extent and variety of the means which may be necessary" to address them.[166] In doing so, however, deliberation must also attend to Madison's warning that concerns about security can skew decisionmakers' judgment, enhancing the appeal of means that may be "inauspicious to . . . liberties."[167] President Obama captured the fine balance required, noting that "there is an inevitable bias . . . within the intelligence community . . . [and] among all of us who are responsible for national security, to collect more information about the world, not less."[168]

In deliberating about the scope of national security surveillance, secrecy is a double-edged sword. As the European Court of Human Rights acknowledged some time ago, some level of secrecy is necessary for surveillance programs.[169] A program that requires too much detail about the bases for surveillance will allow terrorists to adapt their behavior, operating just below the threshold that triggers government scrutiny.[170] Since detailed public disclosure would materially impair surveillance's operational effectiveness, it would also limit the choices available to decisionmakers. Limiting options eviscerates the opportunity for deliberation itself, removing choices that are otherwise sound, and forcing decisionmakers to select choices that are inferior.[171]

However, secrecy can also enable hasty unilateral action. Consider the blowback occasioned by the disastrous CIA-sponsored Bay of Pigs episode. That ill-fated invasion of Cuba by anti-Castro émigrés would not have come to pass if policymakers had been obliged to publicly disclose their plans in advance.[172] While hindsight is always 20/20, it

165. *See* Arendt, *supra* note 12, at 242.

166. *See* The Federalist No. 23, *supra* note 12, at 153 (Alexander Hamilton) (emphasis omitted).

167. *See* The Federalist No. 41, *supra* note 12, at 257–58 (James Madison).

168. *See* Obama, *supra* note 1.

169. *See* Weber v. Germany, App. No. 54934/00, 2006-XI Eur. Ct. H.R. 1173.

170. *See* Kennedy v. United Kingdom, App. No. 26839/05, ¶ 108, Eur. Ct. H.R. (2010).

171. *Cf.* Sissela Bok, Secrets: On the Ethics of Concealment and Revelation 175 (Vintage Books 1989) (1983) (noting argument that, "[i]f administrators had to do everything in the open, they might be forced to express only safe and uncontroversial views, and thus to bypass creative or still tentative ideas").

172. *Cf.* Stephen M. Griffin, Long Wars and the Constitution 113 (2013) (blaming the Bay of Pigs debacle on flawed structure of national security decisionmaking, while asserting that U.S. public opinion would have supported even more aggressive posture toward Cuba); Michael J. Glennon, *National*

seems safe to argue that the United States would have been better off had those plans been disclosed. In such situations, requiring public disclosure would serve as a kind of pre-commitment device for winnowing out bad policy options. Moreover, in many national security contexts, including the warrantless surveillance of the Vietnam Era[173] and the "enhanced interrogation techniques" used by the United States in the eighteen months after September 11,[174] secrecy can mask measures that violate rights under international and/or domestic law.

The Framers sought to manage secrecy with the familiar architecture of separation of powers.[175] Madison designed three branches with powers that overlapped, deterring unilateral action by any branch.[176] The difficulty of acting unilaterally would logically reduce interbranch secrecy, since the effort to persuade another branch would usually involve disclosure of information. The necessity of persuading another branch would also have a useful ex ante effect on intrabranch decisionmaking. Hamilton, opining on the virtues of judicial review, extolled its ability to save the political branches from the perils of precipitous action.[177] Judicial review, for Hamilton, would enhance deliberation, since the political branches would be obliged to factor in the effects of judicial scruples on political initiatives.[178]

Over 150 years after the Constitution's enactment, Justice Jackson described the Constitution's architecture of deliberation between the branches.[179] In his concurrence, Jackson tied the deference due the President to the degree of interbranch deliberation that the President has invited and received. A court, according to Jackson, should accord the President maximum deference when she acts consistently with Congress's will, some deference when the executive acts against the

---

Security and Double Government, 5 HARV. NAT'L SEC. J. 1, 49–50 (2014) (asserting that several justices of the Supreme Court have backgrounds touching on national security that incline them to extend undue deference to unilateral executive action on foreign affairs and national security).

173. *See* PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMC'NS TECHS., *supra* note 30, at 54–55.

174. *See* PETER MARGULIES, LAW'S DETOUR: JUSTICE DISPLACED IN THE BUSH ADMINISTRATION 59–66 (2010); DAVID LUBAN, LEGAL ETHICS AND HUMAN DIGNITY 162, 176–80, 200–02 (2007); Kathleen Clark, *Ethical Issues Raised by the OLC Torture Memorandum*, 1 J. NAT'L SEC. L. & POL'Y 455 (2005); *cf.* Michael L. Kramer & Michael N. Schmitt, *Lawyers on Horseback? Thoughts on Judge Advocates and Civil-Military Relations*, 55 UCLA L. REV. 1407 (2008) (noting military lawyers' opposition to such policies).

175. *See* STANLEY ELKINS & ERIC MCKITRICK, THE AGE OF FEDERALISM 9 (1st ed. 1993) (discussing the Framers' debt to the English concept of three orders of government, that is, monarch, lords, and commons).

176. *See* THE FEDERALIST NO. 51, *supra* note 12, at 322 (James Madison).

177. *See* THE FEDERALIST NO. 78, *supra* note 12, at 469 (Alexander Hamilton).

178. *Id.* at 470.

179. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring).

backdrop of legislative silence,[180] and minimal deference for decisions that defy congressional will.[181]

Both section 215 and section 702 fit squarely into Jackson's first category. In each case, Congress provided for some measure of review by the FISC accompanied by legislative oversight. That interbranch conversation produced the metadata program, including the definition of relevance offered by the FISC, and programs under section 702.

As one would expect from a reasoned interbranch conversation, each program was tailored, particularly in the area of restrictions imposed by both the FISC and the NSA on analysts' access to and use of data collected. For "about" collection under the Upstream program,[182] the FISC required the use of strong selectors keyed to producing foreign intelligence information. Under section 215, the FISC required that analysts use identifiers tied to terrorism to query the metadata collected.

Critics assailed the scope of collection approved by the FISC under section 215 and, to a lesser extent, section 702.[183] However, they failed to adequately address the importance of the use restrictions that the FISC imposed. Similarly, critics condemned the programs' secrecy, but failed to reckon with the benefits of secrecy recognized by the Framers and by subsequent case law and legislative-executive branch dialogue.[184] Understanding the benefits of secrecy is an essential part of the context for interpreting both section 702 and the pre-Snowden version of section 215.

B. Secrecy in American Law

In national security and foreign affairs, secrecy's benefits for deliberation and strategic advantage have been an overarching theme since the United States declared its independence. Indeed, the case law sometimes fails to recognize secrecy's costs.[185] This Subpart's examination of secrecy's role is, in part, a descriptive exercise not connoting endorsement of the case law, but painting a landscape that Congress could plausibly have considered in enacting section 215 and section 702. Because programs under these provisions approved by the

---

180. Dames & Moore v. Regan, 453 U.S. 654, 688 (1981); Curtis A. Bradley & Trevor W. Morrison, *Historical Gloss and the Separation of Powers*, 126 Harv. L. Rev. 411, 415 (2012).

181. *See* David J. Barron & Martin S. Lederman, *The Commander in Chief at the Lowest Ebb—Framing the Problem, Doctrine, and Original Understanding*, 121 Harv. L. Rev. 689 (2008) (analyzing *Youngstown*'s implications).

182. PCLOB Section 702 Report, *supra* note 31, at 36.

183. *See, e.g.*, Donohue, *supra* note 6, at 821; Donohue, *supra* note 8 (manuscript at 58).

184. *See, e.g.*, Sagar, *supra* note 14, at 16–30; United States v. Reynolds, 345 U.S. 1, 9–12 (1953).

185. *Cf.* Adam M. Samaha, *Gov't Secrets, Constitutional Law, and Platforms for Judicial Intervention*, 53 UCLA L. Rev. 909, 933–41 (2006) (discussing case law).

FISC build in greater constraints, they should *a fortiori* be seen as reasonable constructions of their authorizing statutes.

1. Secrecy and the Framers

Although the Framers did not view secrecy as the norm, they found it to be a useful exception.[186] Secrecy could create a corrosive distrust between the people and their representatives, the Framers recognized. On the other hand, secrecy was essential for the performance of some important governmental functions.[187]

George Washington recognized, during the war for independence from the United Kingdom, that, during armed conflicts, secrecy was a necessary ingredient of tactical success. General Washington acknowledged this in a letter to a subordinate ordering reconnaissance in preparation for a possible attack on British forces.[188] After noting the "necessity of . . . procuring good . . . Intelligence," Washington cautioned his subordinate to "keep the whole matter as secret as possible."[189] Explaining the need for secrecy, Washington advised that, "[U]pon secrecy, success depends in most Enterprises of the kind, and for want of it, they are generally defeated, however well planned and promising."[190]

As the heady days of independence lapsed into the chaos of the Articles of Confederation era, Washington and other prominent individuals convened together in Philadelphia under cloak of secrecy to draft a federal constitution. While the Congress had authorized the constitutional convention, the delegates ordered the secretary for the convention to deliver all records of the proceedings to Washington, who had presided over the gathering.[191] The delegates apparently worried that the unvarnished debates in Philadelphia might prejudice public sentiment against the Constitution's enactment, or perhaps embarrass the delegates who toiled there.[192]

The Constitution itself mandated greater transparency, requiring both the House and Senate to "keep a Journal of [their] Proceedings."[193]

---

186. *See* SAGAR, *supra* note 14, at 16–30.

187. *Id.*

188. Letter from George Washington to Colonel Elias Dayton (July 26, 1777), *in* 8 THE WRITINGS OF GEORGE WASHINGTON FROM THE ORIGINAL MANUSCRIPT SOURCES, 1745–99, 478–79 (John C. Fitzpatrick ed., 1933).

189. *Id.*

190. *Id.* at 479.

191. Max Farrand, *Introduction to* 1 RECORDS OF THE FEDERAL CONVENTION OF 1787, at xi, xi (Max Farrand ed., 1st ed. 1911).

192. Not for the last time, the value of secrecy may have been overstated: the papers of the Convention were not published until thirty years later, after President Monroe delegated the task to then Secretary of State John Quincy Adams. *Id.* at xii.

193. U.S. CONST. art. I, § 5, cl. 3; *cf.* Pozen, *Deep Secrecy*, *supra* note 10, at 293–94 (discussing text and background of Journal Clause).

However, that transparency was not absolute. The Journal Clause also permitted the House and Senate to, at their discretion, exempt from publication portions of the proceedings that "require Secrecy."[194] James Wilson of Pennsylvania argued, in a presaging of the fallout from the Snowden disclosures, that secrecy could erode strategic advantages, lending ammunition to those suspicious of the idea of a federal constitution.[195] However, a majority of delegates disagreed, keeping both the express provision for congressional transparency and the exception.[196]

Alexander Hamilton, writing as Publius, also recognized the importance of secrecy. Praising the presidency's potential virtues, Hamilton listed decisiveness, "secrecy," and "dispatch" as cardinal benefits derived from a single chief executive.[197] John Dickinson, addressing delegates to the Constitutional Convention, presaged these sentiments, noting the importance of executive "[s]ecrecy, vigor, and despatch."[198] Dickinson also agreed with Hamilton's wariness about a plural executive, asserting the importance of locating "responsibility" within one person who could then be judged by his display of these virtues.[199]

Hamilton and Dickinson's mating of secrecy and the virtues of a single chief executive gave rise to another mainstay of constitutionalism in practice: a tendency to accord some deference to the President's positions, particularly in foreign affairs. According to Dickinson, the "responsibility" to the people lodged in the President required a measure of deference, since it would be illogical to make a single executive answerable to the people or to other institutions of government without giving the executive the tools to "discharge its functions."[200] This measure of deference need not translate into a sweeping view of the President's power.[201] As I have suggested in a previous Article, the President's authority in a constitutional republic will often be provisional and interstitial, filling gaps based on a reasonable belief that such action

194. U.S. CONST. art. I, § 5, cl. 3.

195. 2 RECORDS OF THE FEDERAL CONVENTION OF 1787, at 260 (Max Farrand ed., 1st ed. 1911) (asserting that allowing any exception to transparency "would furnish the adversaries of . . . reform with a pretext by which weak & suspicious minds may be easily misled").

196. *Id.*

197. *See* THE FEDERALIST No. 70, *supra* note 12, at 523 (Alexander Hamilton).

198. 1 RECORDS OF THE FEDERAL CONVENTION OF 1787, *supra* note 191, at 140.

199. *Id.*

200. *Id.*

201. *See* Curtis A. Bradley & Martin S. Flaherty, *Executive Power Essentialism and Foreign Affairs*, 102 MICH. L. REV. 545, 551–52 (2004) (rejecting the view that the Vesting Clause, U.S. CONST. art. II, § 1, cl. 1, grants the president broad residual authority over foreign affairs).

preserves Congress's ability to deliberate.[202] Secrecy will often be a useful aid in that effort.

2. Secrecy and the Courts

This synergy between deliberation, strategic advantage, and deference to the executive also plays out in case law involving government secrecy. Consider *Totten v. United States*,[203] in which the Supreme Court fashioned an early version of the state secrets doctrine[204] in the course of mandating dismissal of a lawsuit seeking payment for services allegedly rendered by a clandestine Union operative during the Civil War.[205] The Supreme Court worried that in the absence of a state secrets doctrine, an unscrupulous plaintiff could hold up the government for additional money by threatening to divulge sensitive information.[206] In heading off this threat, the Court recognized that secrecy was necessary in both war and foreign relations, and that an expectation of secrecy would prompt reliance by policymakers.[207] Writing for the Court, Justice Field asserted that litigation of disputes over the terms of secret missions would risk exposure of such sensitive dealings, "to the serious detriment of the public."[208] Detriment would flow not merely from disclosure of sources and methods, but from a narrowing of the choices available to government.[209] As Justice Field explained, the risk of exposure attendant on litigation would effectively make clandestine operations "impossible."[210] Courts have found, for similar reasons, that a privilege protects communications that assist the President's deliberations.[211]

---

202. *See* Peter Margulies, *Taking Care of Immigration Law: Presidential Stewardship, Prosecutorial Discretion, and the Separation of Powers*, 94 B.U. L. REV. 105, 131–33 (2014); *cf.* HAROLD HONGJU KOH, THE NATIONAL SECURITY CONSTITUTION: SHARING POWER AFTER THE IRAN-CONTRA AFFAIR 78–79 (1990) (as an example of this interstitial view, observing that President Washington, in announcing his Neutrality Proclamation declaring the United States neutral between France and Britain, "expressly conceded that Congress had the power to change neutrality policy by legislation").

203. 92 U.S. 105 (1875).

204. *See* Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 GEO. WASH. L. REV. 1249, 1277 (2007).

205. *Totten*, 92 U.S. at 105–07.

206. *Id.* at 106.

207. *Id.* (noting that the doctrine would be relevant in any case concerning "secret employments of the government in time of war, or . . . matters affecting our foreign relations, where a disclosure of the service might compromise or embarrass our government in its public duties").

208. *Id.* at 106–07.

209. *Id.*

210. *Id.* at 107.

211. United States v. Nixon, 418 U.S. 683, 705–06, 708 (1974). No privilege is absolute; parties who use the cloak of privilege to commit fraud or other criminal acts will not have their contrivances shielded from disclosure. *Cf. id.* at 707 (arguing that the needs of courts in criminal proceedings outweighed arguments in favor of executive privilege). Deliberation that furthers criminal conspiracies does not serve

Federal personnel cases over a century after *Totten* reveal a similar respect for the manner in which secrecy protects both executive and legislative options. In *Haig v. Agee*, the Supreme Court upheld the State Department's revocation of the passport of an ex-CIA agent who had previously traveled abroad to disclose the names of U.S. intelligence operatives.[212] In upholding the President's action, the Court noted that the action enforced the confidentiality agreement that Agee had agreed to in accepting a federal position. The President's enforcement of the contractual confidentiality agreement served deliberation in two ways. Without power to take such action, a President would have been vulnerable to extortion from unscrupulous ex-employees. To avoid negotiating with every ex-employee, agencies might limit consultation with their own personnel, which undermines deliberation.[213]

The President's action in *Agee* also preserved Congress's opportunity to deliberate. In 1982, Congress expanded enforcement of confidentiality agreements with a criminal statute that prohibited the knowing disclosure of a CIA agent's identity.[214] If the President had not thwarted Agee's plan, the ex-agent's disclosures would have injured U.S. intelligence operations before Congress had an opportunity to act. The President's action thus preserved Congress' ability to pass effective legislation.

Deference to the President on the cost of disclosure also drove the Court's decision in *Department of the Navy v. Egan*.[215] In limiting judicial review of the government's denial of a security clearance to a federal employee to an inquiry into whether the government followed fair procedures, the Court noted the "sensitive and inherently discretionary" nature of decisions to grant security clearances.[216] Justice Blackmun's opinion for the Court asserted that this power flowed, not from any "explicit congressional grant," but instead from the

---

the public. The contours of the privilege recognize that, apart from this exception, impeding an individual or entity's resort to deliberation with counsel would disserve the public interest. *Id.* at 709–10.

212. 453 U.S. 280, 280–85 (1981). Some agents were attacked after these disclosures. *Id.* at 285. Agee's disclosures also violated his contract with the government, which required him to submit public statements regarding his activities to the government for preclearance, and barred him from disclosing confidential information. *Id.* at 284; *see* United States v. Snepp, 444 U.S. 507, 515–16 (1980) (upholding the enforcement of such contracts). *But see* KOH, *supra* note 202, at 140 (critiquing *Agee* as giving short shrift to free speech).

213. United States v. Morison, 844 F.2d 1057, 1083 (4th Cir. 1988) (Wilkinson, J., concurring) (observing that without the ability to enforce confidentiality agreements through prosecutions under the Espionage Act, "[v]ital decisions and expensive programs set into motion by elected representatives would be subject to summary derailment at the pleasure of one disgruntled employee").

214. Intelligence Identities Protection Act of 1982, 50 U.S.C. § 421(a) (1982) (providing for up to ten years imprisonment for person who violates Act).

215. 484 U.S. 518, 530 (1988).

216. *Id.* at 527.

"constitutional investment of power in the President."[217] Justice Blackmun painstakingly detailed the long-standing efforts of the executive to protect sensitive information.[218] He alluded specifically to the formation of the NSA after World War II.[219] According to Justice Blackmun, the "[p]redictive judgment" involved in assessing both whether someone should receive a clearance and the danger if an individual failed to comply with a clearance's terms is inherently an "inexact science," requiring a measure of deference to agency decisionmaking.[220] Justice Blackmun attributed this same view to Congress, even though the statute establishing a scheme for adjudicating matters concerning civil service employment did not expressly preclude more searching review.[221]

As another example of how secrecy and deliberation intersect in Congress, consider the authorization of covert action under Title 50 of the U.S. Code.[222] Congress has authorized covert action, in broad and general terms, to aid the government's deliberation about policy options. The statute permits the President to find that covert action abroad serves U.S. foreign policy goals and to order action based on that finding, subject to oversight by congressional intelligence committees.[223] There are limits to that authority: the President cannot use a covert action finding to order "traditional . . . military activities," such as a significant, ongoing deployment of armed forces abroad.[224] Moreover, the United States appears to accept that any activities involving the targeted use of lethal force abroad must be consistent with international law on the use of force and the conduct of armed conflict.[225] However, a range of activities is permissible, including actions that fall short of an "armed attack" on another state forbidden by the U.N. Charter but nonetheless interfere with that state's sovereignty in ways that would violate

---

217. *Id.*

218. *Id.* 527–28.

219. *Id.* at 527.

220. *Id.* at 529.

221. *See id.* at 531 n.6 (citation omitted). *But see* Deborah N. Pearlstein, *After Deference: Formalizing the Judicial Power for Foreign Relations Law*, 159 U. PA. L. REV. 783, 851 (2011) (arguing against undue deference to the executive branch). *See generally* Robert M. Chesney, *National Security Fact Deference*, 95 VA. L. REV. 1361 (2009) (analyzing the factors driving judicial deference to executive decisions).

222. 50 U.S.C. § 3093 (2014); *cf.* Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 5 J. NAT'L SEC. L. & POL'Y 539, 540–45 (2010) (discussing the differences and similarities between covert action and military operations).

223. 50 U.S.C. § 3093(b)(1) (2014) (requiring that the President keep intelligence committees "fully and currently informed of all covert actions").

224. *Id.* § 3093(e)(2).

225. *See* Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, Keynote Address at the Annual Meeting of the American Society of International Law: The Obama Administration and International Law (Mar. 25, 2010), *available at* http://www.state.gov/s/l/releases/remarks/139119.htm.

international law.[226] Covert action authority expands the options available, since many activities the President can order based on a covert action finding would be effectively precluded if the United States was obliged to publicly acknowledge them.[227]

The covert nature of the activities undertaken can also pose challenges for deliberation.[228] The ability to authorize actions without public debate can allow "groupthink" to operationalize bad ideas.[229] This was the case, for example, with U.S. policy toward Iran in the 1950s and Latin America and the Caribbean in the 1960s and 1970s.[230] Groupthink also plagued the Bush administration's TSP, which lacked the statutory grounding and judicial and legislative oversight of the metadata program.[231] My object here is not to defend particular policies. Rather, I aim only to demonstrate that Congress has regularly used vague terms such as "covert action" and narrower forms of oversight, such as reporting to the intelligence committees, to widen the range of policy options available in the national security space. A broader reading of section 215's relevance standard, coupled with both intelligence committee oversight and court review, would be consistent with Congress's desire to broaden policy options.

3. Technology, Secrecy, and National Security

The courts have also tended to show deference to government decisions on technology and national security. In granting this deference, courts have recognized that a failure to show deference could confine technology to the status quo, chilling innovation.[232] Moreover, courts have recognized that requiring public disclosure of surveillance methods

---

226. Jules Lobel, *Covert War and Congressional Authority: Hidden War and Forgotten Power*, 134 U. PA. L. REV. 1035, 1040 (1986).

227. *Id.* at 1078.

228. *See* GRIFFIN, *supra* note 172, at 103–04.

229. *See* Chesney, *supra* note 221, at 1414–16 (2009); Oren Gross, *Chaos and Rules: Should Responses to Violent Crises Always Be Constitutional?*, 112 YALE L.J. 1011, 1029–30, 1035–37 (2003); Peter Margulies, *Judging Myopia in Hindsight:* Bivens *Actions, National Security Decisions, and the Rule of Law*, 96 IOWA L. REV. 195, 204–11 (2010).

230. *See* Lobel, *supra* note 226, at 1056–57.

231. *See* Kathleen Clark, *The Architecture of Accountability: A Case Study of the Warrantless Surveillance Program*, 2010 B.Y.U. L. REV. 357, 394–95; Heidi Kitrosser, *It Came from Beneath the Twilight Zone: Wiretapping and Article II Imperialism*, 88 TEX. L. REV. 1401, 1406–11 (2010). President Franklin Roosevelt ordered wiretapping of suspected spies in the lead-up to America's entry into World War II. *See* Neal Katyal & Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent*, 60 STAN. L. REV. 1023, 1049–54 (2008). The secretive and convoluted nature of this effort make it a doubtful precedent for the TSP. *Id.* at 1062–70. By the same token, the metadata program's legality does not hinge on assessments of the lawfulness of either Roosevelt's surveillance initiative or the TSP, since in section 215 Congress expressly empowered the FISC to approve surveillance requests from the executive branch. *Id.* at 1029–32.

232. *See, e.g.*, Chevron, U.S.A., Inc. v. Natural Res. Def. Council, 467 U.S. 837, 863 (1984).

would allow terrorists and other adversaries to "adapt" to those methods and thereby evade detection.[233] In addition, courts have viewed technological advances as a shield as well as a sword, possessing the potential to *enhance* privacy and enable curbs on government overreaching.[234]

The courts' deference to the executive branch on technology was evident in the Supreme Court's canonical decision on deference to agencies, *Chevron, U.S.A., Inc. v. Natural Resources Defense Council*.[235] Often, courts defer because of agencies' superior expertise. As the *Chevron* Court noted in deferring to an agency policy on ways to reduce air pollution, an agency construes a statute, "not in a sterile textual vacuum, but in the context of implementing policy decisions in a technical and complex arena."[236] That complexity makes it far more risky and cumbersome for courts to either second-guess agency decisions developed over time by experts or to require express authorization from Congress for new technologies.

The first point here is most obvious: Executive agencies have access to information on a far broader scale than courts.[237] Courts that second-guess agencies risk getting it wrong.

The second point requires more unpacking. Requiring express authorization from Congress obliges executive branch officials to repeatedly return to Congress for permission to employ new technology. That requirement has some advantages for deliberation and individual rights, but it also has two key drawbacks: (1) in the national security field, it increases the risk that some technological advances will be disclosed before it is in the United States' interest to disclose them, and (2) it makes the implementation of new technology far more unwieldy.

Two important cases on secrecy illustrate the first problem. In *United States v. Reynolds*, the Supreme Court held that the government could invoke the state secrets privilege to shield an accident report prepared by the Air Force on the crash of a B-29 bomber in litigation brought by the widows of the victims.[238] At the time of the accident, the bomber in question was testing an early version of a "pilotless aircraft guidance system,"[239] although the documents that the plaintiffs requested

---

233. *See* Kennedy v. United Kingdom, App. No. 26839/05, ¶ 140, Eur. Ct. H.R. (May 18, 2010).

234. *See, e.g.*, *In re* Prod. of Tangible Things from [Name Redacted by the Court], No. BR 08-13, 2009 WL 9150913, at *9–10 (FISA Ct. Mar. 2, 2009).

235. 467 U.S. 837 (1984).

236. *Id.* at 863.

237. *Cf.* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 980 (2005) (observing that, when compared with courts, agencies are "better equipped to make . . . difficult policy choices").

238. 345 U.S. 1, 9–12 (1953).

239. *See* David Rudenstine, *The Irony of a Faustian Bargain: A Reconsideration of the Supreme Court's 1953* United States v. Reynolds *Decision*, 34 CARDOZO L. REV. 1283, 1300 (2013).

contained no mention of this aspect of the case.[240] The government alleged that disclosure of the accident report was "prejudicial to the efficient operation" of the Air Force, "not in the public interest," and "inconsistent with national security."[241] The Supreme Court agreed that the government could decline to disclose the documents, which in fact merely listed tragically mundane errors in aircraft maintenance.[242] Rejecting the plaintiffs' claim that *in camera* review of the accident report would suffice to determine whether it contained references to sensitive information, the Court asserted that even disclosure to a judge could result in compromising sources and methods.[243] Noting that "new[] . . . electronic devices have greatly enhanced the effective use of air power," the Court opined that "electronic devices must be kept secret if their full military advantage is to be exploited in the national interests."[244] The Court declined to order production of the accident report, finding a "reasonable danger that the accident investigation report would contain references to the secret electronic equipment which was the primary concern of the mission."[245]

A second decision that refined the Court's approach to secrecy, technology, and deference is *CIA v. Sims*.[246] In *Sims*, on which Judge Kollar-Kotelly relied in her FISC opinion on Internet metadata, the Supreme Court upheld denial of a Freedom of Information Act ("FOIA") request on grounds that even a seemingly innocuous disclosure might form part of a "mosaic" that could reveal intelligence sources and methods to U.S. adversaries.[247] The *Sims* Court warned that, "what may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned

240. *Id.* at 1342–43.

241. *Id.* at 1342. These allegations were aggressive if not knowingly misleading. *Id.* at 1356–57.

242. *See* STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 158 (5th ed. 2011).

243. United States v. Reynolds, 345 U.S. 1, 10 (1953).

244. *Id.*

245. *Id.* Here, as with discussion of *Department of the Navy v. Egan*, *supra* note 108, my point is not to praise the Supreme Court's decision. The plaintiffs in *Reynolds* had strong arguments, although it is telling that reviewing courts in this century, having full knowledge of the documents in question, have declined to revisit the Supreme Court's decision. In a 2005 decision declining to open up the litigation on grounds that the government had engaged in misrepresentation, the Third Circuit deferred to the government's position that its earlier representations were not false because even the mundane information in the accident report could have comprised part of a "mosaic" that was useful to U.S. adversaries. Herring v. United States, 424 F.3d 384, 391 n.3 (3d Cir. 2005) (suggesting that public disclosure of the accident report could have revealed the content of training missions, the unit involved, and the capability of the aircraft in the mission, such as the ability to operate at high altitudes); *cf.* Weinberger v. Catholic Action of Hawaii, 544 U.S. 139 146–47 (1981) (holding that the Court lacked power to compel an environmental impact statement for a Navy facility that might store nuclear weapons, in part because of need for secrecy on weapons' location).

246. 471 U.S. 159 (1985) (cited in Kollar-Kotelly Opinion, *supra* note 48, at 30 n.24).

247. *Id.* at 177.

item of information in its proper context."[248] Judicial deference was therefore appropriate in assessing the intelligence assessments of the executive, which "must of course be familiar with 'the whole picture,' as judges are not."[249] Such deference was particularly appropriate, the *Sims* Court concluded, "given the magnitude of the national security interests and potential risks at stake."[250]

The *Sims* Court's mosaic theory, with its stress on judicial deference on secrecy, was a reference point for Senator Kyl in discussing the 2006 amendments to section 215. Discussing limits in the bill on telecommunications companies' disclosure of government requests for information, Kyl explained the need for a measure of deference to the executive branch's choices:

> The standard in the conference report . . . recognizes that sensitive national security and diplomatic relations judgments are particularly within the Executive's expertise. The Constitution has vested these determinations with the Executive, and courts have long recognized that judges are ill-suited to be second-guessing the Executive's national security and diplomatic affairs judgments. Disclosures that seem innocuous to a judge who . . . must view those disclosures without being fully aware of the many other data points known to our enemies—may nonetheless be quite damaging.[251]

Obliging agencies to return to Congress every time they encounter a new technology can also stifle innovation. In today's world, technological change occurs at an astronomical rate.[252] Ponder the pitiable fate of the Blackberry, hailed as cutting edge technology in one decade and nearing collapse less than fifteen years later.[253] Even modest alterations in technology can render a regulatory regime ready for mothballs.[254] Requiring a trip to Congress for fresh amendments every time technological change mooted out a previously effective regulatory framework would leave regulators playing Sisyphus. The agency would

---

248. *Id.* at 178; *cf.* David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005) (discussing the rationale for the mosaic theory).

249. *Id.* at 179.

250. *Id.*; *see* Pozen, *Deep Secrecy*, *supra* note 10, at 304–05 (discussing case law upholding secrecy). The Court has also invoked the need to preserve secrecy as a basis for denying standing to challenge FISA provisions. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1149 n.4 (2013) (expressing concern that allowing standing without proof of direct harm would "allow a terrorist . . . to determine whether he is currently under U.S. surveillance simply by filing a lawsuit challenging the Government's surveillance program").

251. 152 CONG. REC. S2437-38 (daily ed. Mar. 2, 2006) (statement of Sen. Kyl).

252. *See* Yochai Benkler, *Open Wireless vs. Licensed Spectrum: Evidence from Market Adoption*, 26 HARV. J.L. & TECH. 69, 94 (2012) (discussing Moore's Law, named after one of the founders of the Intel Corporation, which holds that the speed and capacity of computing technologies doubles every two years).

253. *See* Ian Austen, *BlackBerry Staggers to a Deeper, $4.4 Billion Loss*, N.Y. TIMES, Dec. 21, 2013, at B1.

254. *See* Jonathan Masur, *Judicial Deference and the Credibility of Agency Commitments*, 60 VAND. L. REV. 1021, 1028 (2007).

eagerly draft regulations pursuant to a current statutory authorization, only to find that technological change had rendered those rules old before their time, requiring further legislative activity before starting work on a new batch of regulations.[255] The cycle would then repeat itself. Such adventures in futility would seem quixotic were they not dangerous. If adaptability is a watchword for administrative law, allowing counterterrorism techniques to lag behind technology in smart phones or washing machines seems perverse.[256]

However, concern about individual rights requires some limits on the government's ability to use new technology in information gathering. Consider the dynamic world of data analytics. Through the 1980s, much analysis of data required teams of workers engaged in reading and digesting documents.[257] Law firms and other concerns that used this technique billed clients for thousands of hours. In the last twenty-five years, data analysis has shifted to the use of keywords for searching documents electronically.[258] The last fifteen years have seen substantial advances in computerized coding of huge document sets. Predictive coding uses a "seed set" of documents that analysts compile using keywords. The seed set "trains" software that enables a computer to find documents relevant to a lawsuit in a much larger set.[259] While the adoption of this technology is still gathering steam in civil litigation, data aggregators in the private retail sector have forged ahead in training software to draw connections between Internet consumers' search patterns, personal data (such as residence or computer ownership), and purchasing and borrowing proclivities.[260] Advanced data analytics can be dystopian, giving major corporations or government too large a window on individuals' habits and commitments.[261] Use of such data mining

255. *Id.*

256. *But see* Kerr, *supra* note 155, 26–30 (arguing for requiring express congressional authorization of new technology).

257. For a balanced analysis of data analytics compared with hard copy research on the history of cinema, see Richard Abel, *The Pleasures and Perils of Big Data in Digitized Newspapers*, 25 FILM HIST. 1, 2 (2013) (noting that analyzing databases of newspapers yielded information that would have been far more difficult to obtain from print sources about the popularity of pro-German movies in America before U.S. entry into World War I).

258. *In re* Grand Jury Subpoena Duces Tecum, 846 F. Supp. 11, 13 (S.D.N.Y. 1994) (noting that "relevant documents can be isolated through key-word searching," so there was no need to produce the entire "computer storage device").

259. *See* Da Silva Moore v. Publicis Groupe, 287 F.R.D. 182, 186–87 (S.D.N.Y. 2012); *cf.* John Didday, *Informed Buyers of E-Discovery: Why General Counsel Must Become Tech Savvy*, 5 HASTINGS SCI. & TECH. L.J. 281, 303–05 (2013) (discussing the promise of advanced machine learning in e-discovery).

260. *See* Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2021–22 (2013).

261. *See* Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1919–27 (2013); *cf.* Dahlia Lithwick & Steve Vladeck, *Taking the "Meh" out of Metadata: How the Government Can Discover Your Health Problems, Political Beliefs, and Religious Practices Using Just Your Metadata*, SLATE (Nov. 22, 2013),

methods to identify suspected terrorists from bulk metadata could be problematic, particularly in the domestic realm.[262] Methods of this kind should require express congressional approval. Fortunately, in this respect the uses of technology approved by the FISC for metadata queries appear quaint, relying on simple identifiers, such as phone numbers.

C. Technological Innovation Can Both Enhance and Check the Power of Surveillance

Conceding that some technological innovations in surveillance *would* require a return visit to Congress, we can ask whether the FISC is capable of holding that line. Although the initial implementation of the metadata program has spurred critics' doubts, the FISC's overall track record suggests that it is capable of robust review. The FISC's efforts are aided by the two-sided character of technological change. The first and more obvious aspect is the intrusive power of new technologies. The second more subtle element is the dynamic ability to devise technological safeguards *against* intrusions. Focusing only on the first aspect distorts law and policy. In contrast, a balanced approach permits orderly development of technology while still preserving privacy rights and Congress's opportunity to deliberate about quantum leaps in surveillance capabilities.

Courts have striven for a balanced approach in regulating digital searches that seeks neither to stifle nor surrender to "[r]apid changes in the dynamics of communication and information transmission itself."[263] In *City of Ontario v. Quon*, the Supreme Court adopted a balanced approach to an employer's investigation of employee texting, observing that "[p]rudence counsels caution . . . [lest] facts . . . are used to establish far-reaching premises."[264] The Court opted for a narrow holding based on the employer's legitimate interest in ascertaining whether a contract

---

http://www.slate.com/articles/news_and_politics/jurisprudence/2013/11/nsa_and_metadata_how_the_government_can_spy_on_your_health_political_beliefs.html (discussing the potential for invasions of privacy by the government).

262. *See* United States v. Maynard, 615 F.3d 544, 561–63 (D.C. Cir. 2010) (using the "mosaic" concept not as justification for government secrecy, as in CIA v. Sims, 471 U.S. 159 (1985), but as test for when government aggregation of information about individuals' non-private activities might reveal more than information about any one activity, thus violating an individual's reasonable expectation of privacy and triggering Fourth Amendment protection); United States v. Jones, 132 S. Ct. 945 (2012); *cf.* Orin S. Kerr, *The Mosaic Theory of the First Amendment*, 111 Mich. L. Rev. 311, 345–52 (2012) (raising concerns about whether the mosaic theory is coherent and manageable, particularly in light of rapidly evolving technology); Wayne A. Logan, *"Mosaic Theory" and Megan's Laws*, 2011 Cardozo L. Rev. 95, 96–97 (suggesting a parallel between the mosaic theory and other law enforcement policies, such as mandated disclosures to the government by convicted sex offenders).

263. City of Ontario v. Quon, 560 U.S. 746, 759 (2010).

264. *Id.*

for text messaging services on company-provided pagers resulted in "extensive" personal communications by employees.[265] In finding that the employer, a law enforcement agency, acted reasonably, the Court also cited the tailored nature of the employer's search of employees' text messages, which included only two months of the relevant contractual period.[266]

The pace of technological change does not dictate a pro-government result. After *Quon*, the Supreme Court decided *United States v. Jones*, in which it held that law enforcement officials violated the Fourth Amendment by attaching a GPS device to a suspect's car without a warrant and tracking the car's movements for a month.[267] In *Jones*, Justice Alito's concurrence sounded a warning about technological change that removed practical checks on law enforcement surveillance of an individual's movements.[268] This evolving ease led the Court to restrict GPS surveillance.[269] However, Justice Alito also hinted that restrictions on GPS surveillance in the domain of ordinary criminal law, such as investigations of drug trafficking, might not be wise or constitutionally necessary in areas with greater stakes.[270]

The Court's decision in *Riley v. California*, holding that the "search incident to arrest" doctrine did not permit a warrantless digital search of a defendant's cell phone, also curbs ordinary law enforcement without addressing national security surveillance.[271] In *Riley*, Chief Justice Roberts, writing for a unanimous court, observed that police officers making an arrest should not automatically gain access to the "sum of an individual's private life" contained on today's cell phones.[272] Chief Justice Roberts also noted that the rich "combination" of digital data on an individual's cell phone might yield far more about an individual's "private interests and concerns" than might be apparent from a single record viewed in isolation.[273] Chief Justice Roberts also discounted the value of "'protocols'" developed internally by law enforcement to address the problem of access to additional reams of information stored

265. *Id.* at 761.

266. *Id.*

267. 132 S. Ct. 945, 954 (2012).

268. *Id.* at 963 (Alito, J., concurring) (noting that, "[t]raditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken").

269. However, Justice Alito also acknowledged that technological change could work in the opposite direction, paving the way for "periods in which popular expectations are in flux . . . [n]ew technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile." *Id.* at 962.

270. *Id.* at 964.

271. 134 S. Ct. 2473, 2493–95 (2014).

272. *Id.* at 2489.

273. *Id.* at 2489–90.

on the cloud.[274] Chief Justice Roberts said, damning with faint praise, that this was "[p]robably a good idea," but then tartly noted that "the Founders did not fight a revolution to gain the right to government agency protocols."[275]

However, Chief Justice Roberts limited the implications of this concern about government access to combined data. He noted that the issue arose in *Riley* in the context of a conceded Fourth Amendment search.[276] Nothing in the Court's opinion addresses the legality under the Fourth Amendment of government collection of noncontent data such as call records that an individual has already made available to a third party.

Justice Alito added a concurrence in *Riley* that echoed the concern of legislators like Senator Kyl that technological change also enhanced the capacities of criminals. "Cell phones are of great value for both lawful and unlawful purposes," Justice Alito observed, and "[t]hey can be used in committing many serious crimes."[277] Chief Justice Roberts acknowledged this point in his opinion, agreeing that cell phones are "important tools in facilitating coordination and communication among members of criminal enterprises."[278] For Justice Alito, this suggested that deference to the legislature would be useful in weighing the balance between privacy and law enforcement. As Justice Alito put it, "Legislatures, elected by the people, are in a better position than [courts] . . . to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future."[279] While the core privacy protections built into the Fourth Amendment fully support giving the Court the last word on the immediate question before it in *Riley*, Justice Alito's point underscores the wisdom of Justice Powell's opinion for the Court in *Keith*, which invited Congress to address the difficult issues of national security surveillance. Such deference has even more resonance in the context of U.S. surveillance abroad, where courts have acknowledged that daunting deficits in the ability to gain and analyze data require a measure of deference to the political branches.[280]

In taking the balance between effectiveness and intrusion seriously, courts have often used technological innovation as a means for controlling Fourth Amendment searches of content. For example, courts have inserted search protocols in warrants authorizing law enforcement

274. *Id.* at 2491.
275. *Id.*
276. *Id.* at 2489 n.1.
277. *Id.* at 2497 (Alito, J., concurring).
278. *Id.* at 2493.
279. *Id.* at 2497–98 (Alito, J., concurring).
280. *See, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980).

inspection of laptops that limit the time of inspection, the domains of the computer that law enforcement can access, and even the keywords that law enforcement officials use to conduct their search.[281] Corporations routinely use blocking filters and other technology to limit customers' ability to search online content.[282] Constraints on search protocols allow the court to limit the breadth and intrusiveness of the government's search, and prevent the government from relying on invidious criteria such as political, cultural, or religious views.[283]

This quest for balance in searches of content has important ramifications for noncontent information gathering that Congress believed, based on long-standing Supreme Court precedent, did not raise Fourth Amendment issues.[284] A balanced approach to metadata collection would acknowledge that technological advances, such as blocking filters and analogous controls, can impose meaningful constraints on government data analysts. Filters and other automated controls can prevent a data analyst from gaining access to data without using preapproved key words or other search terms. As in the Fourth Amendment context, judicial review of search requests can require the use of such technical controls.[285] While talented data analysts might try to engineer ways to frustrate these controls, that possibility does not render controls useless. The solution is to build in ways of monitoring such attempts and require training that emphasizes compliance. Courts monitor compliance with search protocols in the Fourth Amendment context, dealing with myriad law enforcement agencies. If compliance is possible there, it should also be possible in the bulk collection of metadata. Congress's inclusion of the provision for FISC review in section 215 suggests that Congress wanted the court to craft conditions

281. *See* United States v. Reeves, Crim. No. 11-520 JBS, 2012 WL 1806164, at *9–11 (D. N.J. May 17, 2012) (holding that keyword searching without date limitation specified in warrant violated Fourth Amendment); *cf.* Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1121–22 (2009) (praising search protocols in laptop searches); Athul K. Acharya, Note, *Semantic Searches*, 63 DUKE L.J. 393, 409–23 (2013) (analyzing search protocols in Fourth Amendment cases).

282. *See* Authors Guild, Inc. v. Google, Inc., 954 F. Supp. 2d 282, 286–87 (S.D.N.Y. 2013) (noting that Google uses technology to limit Google Books searches of certain volumes; to prevent visitors from reading the entire volume, visitors must use the "snippet-view" mode that shows just three excerpts for each search term employed and imposes other restrictions).

283. *See* United States v. Comprehensive Drug Testing, Inc. 621 F.3d 1162, 1173 (9th Cir. 2010) (en banc). A noted scholar who initially favored this development has more recently cautioned that courts have become too wedded to search protocols, which can skew both investigations and the development of the law. Courts considering the lawfulness of digital searches may focus too much on the mechanical issue of whether law enforcement complied with the terms of the search protocol, and less on whether officials acted reasonably. *See* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1255–57 (2010).

284. *See* Smith v. Maryland, 442 U.S. 735, 741–43 (1979).

285. *See In re* Prod. of Tangible Things from [Name Redacted by the Court], No. BR 08-13, 2009 WL 9150913, at *9–10 (FISA Ct. Mar. 2, 2009).

on access to data that would balance privacy and security. The FISC's conditions met this objective.[286]

IV. Metadata in Practice: The 2009 Disclosures Regarding Noncompliance

The deference to the executive described above is a persuasive precedent for the framework in place prior to Snowden's revelations. The data collected by the government is substantial, exceeding in scale, if not in kind, the data acquired in typical subpoenas.[287] Judicial controls are also greater, narrowing access to the data thus acquired. However, the FISC's robust role in enforcing its own controls emerged from a crisis in the program. Moreover, the executive's disclosures to Congress on this crisis barely crossed the adequacy threshold. Here, the dynamic conception must dovetail with reform.

Until the Snowden revelations, metadata's biggest challenge occurred in 2009. In January of 2009, the Justice Department informed the FISC of significant shortfalls in the NSA's compliance with judicial controls.[288] The FISC fashioned stringent remedies, which the NSA has implemented.[289] However, dealing with the substantive problem is only part of the story. Providing the best possible information to Congress is still a work in progress.

Some background on the 2009 issues is helpful. As noted in Part I, the government received approval from the FISC in 2006 to collect metadata concerning phone calls on a rationale similar to the one used by Judge Kollar-Kotelly in 2004 to authorize collection of Internet communications.[290] That approval was conditioned on a requirement that the government query the metadata only with identifiers that were RAS-approved.[291]

There was one substantial problem with implementation of the metadata program from its 2006 FISC authorization to early 2009: the NSA did not fully comply with the FISC's restrictions on identifiers.[292] A Justice Department lawyer brought this compliance issue to the FISC's

---

286. *See infra* notes 298–99 and accompanying text.

287. *Cf.* Kris, *supra* note 59, at 24 (discussing the differences between the scale and scope of traditional subpoenas and the metadata program, respectively).

288. *In re Prod. of Tangible Things*, 2009 WL 9150913, at *4–7.

289. *See In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Name Redacted by the Court], No. BR 13-109, 2013 WL 5741573, at *10–14 (FISA Ct. Oct. 11, 2013).

290. *See In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Name Redacted by Court], No. BR 06-05, 2006 WL 7137486 (FISA Ct. May 24, 2006).

291. *Id.* at *2.

292. *See In re Prod. of Tangible Things*, 2009 WL 9150913, at *4–6; Donohue, *supra* note 6, at 807–08. *See In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, 2006 WL 7137486.

attention in January 2009.[293] Judge Walton of the FISC rightly characterized these compliance issues as substantial, explaining that almost ninety percent of all identifiers used were *not* RAS-approved.[294] Moreover, no lawyer or NSA official had previously disclosed this compliance problem to the court, although many submissions by the government had flatly asserted that the NSA was complying with the 2006 FISC order. Judge Walton suggested that this prolonged period of noncompliance constituted either a willful and substantial "misrepresentation" or a failure of the NSA to even *understand* the FISC's conditions.[295]

Through early 2009, in other words, the metadata program did not reflect the balance between data acquisition, secrecy, and privacy protections that a dynamic framework requires. Critics of the metadata program have argued that the FISC should have simply shut down the program in response to these problems.[296] However, that response would have left a gap in intelligence gathering capabilities that the FISC was rightly reluctant to create.[297] Instead, the FISC imposed relief that remedied noncompliance. For example, for several months in 2009, the NSA had to submit to the FISC for preapproval all requests to designate identifiers, unless an emergency existed.[298] The FISC also ordered the NSA to perform an "end-to-end" review that would diagnose compliance issues and suggest solutions.[299]

While one can argue that as of January 2009, the government disclosed implementation problems to the FISC and took its medicine, whether the executive branch adequately informed Congress is a closer question. The best answer is that the government performed adequately because it informed the intelligence committees of compliance issues and included relevant FISC opinions. Legislators so inclined could read the court decisions and draw their own conclusions. Senator Wyden became an avid student of the FISC's jurisprudence.[300] His persistent criticism of the bulk collection program owed much to information that the executive

293. *See* Donohue, *supra* note 6, at 808; Lizza, *supra* note 10, at 56.

294. *In re Prod. of Tangible Things*, 2009 WL 9150913, at *4 n.2.

295. *Id.* at *6–8.

296. *See* Donohue, *supra* note 6, at 814.

297. *In re Prod. of Tangible Things*, 2009 WL 9150913, at *17 (deciding not to order cessation of metadata collection because of the government's "repeated representations that the collection of . . . [business record] metadata is vital to national security" and "the Court's prior determinations that, if the program is conducted in compliance with appropriate minimization procedures, such collection conforms with 50 U.S.C. § 1861").

298. *See id.* at *18–19; Donohue, *supra* note 6, at 819.

299. *In re Prod. of Tangible Things*, 2009 WL 9150913, at *9–10.

300. *See* Lizza, *supra* note 10, at 60 (reporting that, "Wyden . . . had read the court opinions").

branch had provided.[301] However, the government's own summaries of those FISC decisions were less specific than they should have been.

The government's descriptions of the compliance issues failed to convey the breadth of noncompliance or adequately assess blame. For example, the government disclosed, in late February 2009, to the House Intelligence Committee that in January it had uncovered episodes of noncompliance.[302] The February memorandum did not provide the comprehensive information that is ideal for sound legislative oversight. In the memo, the NSA General Counsel reported cryptically that an "automated alert process" used to query the metadata "did not operate in conformity with the Court's orders."[303] While this characterization was correct, it started a trend that would continue in subsequent disclosures of ascribing failures to automation and letting the humans off the hook.

A December report to the Intelligence Committee also blamed the machines.[304] It ascribed NSA noncompliance to the "implementation of highly sophisticated technology in a complex and ever-changing communications environment which, in some instances, resulted in the automated tools operating in a manner that was not completely consistent with the specific terms of the" FISC's decrees.[305] The report's scapegoating of those pesky "automated tools" obscures far more than it enlightens. Automated search tools function in the report like rogue robots in a 1950s science fiction movie. NSA officials are cast as hapless victims of the robots' revolt. However, despite the sophistication of the NSA's tools, the agency has not taken up residence on the set of the next installment of *Star Trek*. At the NSA, humans are in charge. Indeed, the most puzzling aspect of the December report is its sense that the "rogue robots" narrative was somehow favorable to the agency. After all, if NSA officials lack the competence to handle their own creations, the nation is in far worse trouble than even Edward Snowden believes.

The fault with these memos was not merely the leaden quality of the officials' prose. To best perform oversight, the House Intelligence Committee and its Senate counterpart should have received a fuller summary of the issues. More comprehensive disclosure would have enhanced legislators' capacity to fully assess the risks and benefits of the bulk collection program.[306]

---

301. *Id.*

302. *See* Memorandum from Vito T. Potenza, Gen. Counsel, Nat'l Sec. Agency to Staff Director, House Permanent Select Comm. on Intelligence (Feb. 25, 2009), *available at* http://www.dni.gov/files/documents/501/25%20Feb%2009%20NSA%20CN_SealedFINAL.pdf.

303. *Id.*

304. *See* Weich, *supra* note 38, at 4.

305. *Id.*

306. The discussion in the text may focus unduly on the phrasing of one report. The December 2009 report hints that substantial disclosure may have occurred in other settings, including real-time exchanges with legislators. *Id.* (observing that incidents of noncompliance "were reported . . . in great

That said, the government's repeated acknowledgments of noncompliance were an adequate signal to Congress that something had been amiss. Moreover, by the time of the December 2009 report, the government had reason to believe that it had addressed the problems that the FISC had identified. The December report detailed those steps appropriately. A diligent legislator could have followed up with further requests for information. Some did so at the briefings that the government provided in connection with reauthorization efforts. Clearly Senator Wyden followed up, gaining information that confirmed his belief that bulk collection was contrary to section 215, and a bad idea to boot.[307] While not all legislators followed Senator Wyden's lead, blame for legislative lack of interest should not fall on the executive. Passivity on the part of members of Congress is hardly a new phenomenon, or one confined to section 215 reauthorizations.[308]

However, the lack of specificity in the government's summaries is a red flag that highlights the need for reform. It is disturbing that Congress depended on the executive branch for disclosure, as did the FISC. While the 2009 disclosures elicited robust remedies from the FISC, new problems can arise in the future that the FISC's current safeguards cannot control. More extensive statutory disclosure requirements could ameliorate this risk. For example, the government should be required to provide both an executive summary and an in-depth analysis of each FISC opinion that materially modifies the bulk collection program. It should also be required to provide regular reports to the intelligence

---

detail."). Those real-time conversations are the most effective kind of executive disclosure to the intelligence committees.

307. Lizza, *supra* note 10, at 60.

308. To facilitate a broader view of both section 215 and section 702, I do not address in detail arguments that, by reauthorizing section 215 on two occasions before Snowden's revelations, Congress ratified the FISC's interpretation of relevance. For more discussion of the effects of reenactment, see Lorillard v. Pons, 434 U.S. 575, 580 (1978) (cited in Forest Grove Sch. Dist. v. T.A., 557 U.S. 230, 239–40 (2009)); ACLU v. Clapper, 959 F. Supp. 2d 724, 743–45 (S.D.N.Y. 2013); *cf.* Deborah A. Widiss, *Undermining Congressional Overrides: The Hydra Problem in Statutory Interpretation*, 90 TEX. L. REV. 859, 871–72 (2012) (noting the principle that "Congress intends to incorporate authoritative interpretations of statutory text when it uses language from one statute in a related context"); Einer Elhauge, *Preference-Estimating Statutory Default Rules*, 102 COLUM. L. REV. 2027, 2112–13 (2002) (asserting that, "once the interpretation 'has been fully brought to the attention of the public and the Congress,'" reenactment with other alterations suggests the interpretation is "presumptively correct"). It is worth noting, however, that in 2010, the House and Senate intelligence committees wrote to all of the members of their respective bodies, noting that the executive was offering each member an opportunity to attend a briefing and read a classified report on "important intelligence collection made possible" under section 215. The classified report itself described section 215 as entailing the "production of the business records . . . relating to *substantially all* of the telephone calls" handled by U.S. telecommunications companies. *See Clapper*, 959 F. Supp. 2d at 745 (emphasis added). That information should have alerted a reasonably diligent member of Congress to the stakes involved in reauthorization.

committees on search results.[309] These reforms will fine-tune Congress's discharge of its oversight duties and produce a more effective dynamic collaboration with the executive branch. As we shall see, the difficulties inherent in limited congressional oversight also make a strong case for creation of a public advocate at the FISC.[310]

V. The Dynamic Conception After Snowden

The Snowden revelations have triggered a reevaluation of both section 215 and section 702. After Snowden, national security surveillance programs should have to pass two tests. First, they should be adequately tailored. Second, they should be subject to an optimal mix of internal and external constraints.

Tailoring must include both a nexus to legitimate government interests and protections against targeting the content of U.S. persons' communications. Tailoring is necessary so that government does not gain indiscriminate access, rummaging through the personal data and communications of any individual without a legitimate reason rooted in national security or the conduct of U.S. foreign affairs. The right mix of collection and use restrictions will often be the result of negotiations between the political branches, as in legislative efforts pending as of August 2014 to modify the section 215 program by requiring that the government seek a court order to acquire call records from private companies using a "specific selection term."[311]

Pending legislative reform efforts also enhance the mix of internal and external constraints governing both collection and surveillance by adding a voice to FISC proceedings opposing the government's position and enabling more review of FISC decisions. These reforms seek to temper intelligence agencies' tendency to push the envelope into unduly intrusive areas of use and collection. Some constraint by the courts is appropriate, given the judiciary's role, which was acknowledged by Hamilton in *The Federalist No. 78* as a brake on the passing humors of the political branches. That review may be ex ante or ex post, depending on the context. A public advocate who can promote a robust adversarial process would be helpful in empowering courts. Congressional oversight is also vital.

Each external constraint should complement internal constraints. An institutional compliance culture will include checks on analysts' understandable proclivity to search for more data, whatever the source.

---

309. Heightened disclosure is one feature of a current bill, the FISA Improvements Act of 2013, sponsored by Senator Feinstein of California, that has been approved by the Senate Intelligence Committee. *See* FISA Improvements Act of 2013, S.1631, 113th Cong. (2013).

310. *See infra* note 328 and accompanying text.

311. *See* USA Freedom Act of 2014, S. 2685, 113th Cong. § 103(a) (introduced July 30, 2014).

Those checks should include processes already in place in the intelligence community, including review by senior officials of selectors and other search criteria, particularly queries of content from U.S. persons.

A. Section 215, Metadata, and Specific Selection Terms

Proposed legislation introduced in the Senate in July of 2014 after negotiations between Senator Leahy and government representatives would roll back the metadata program in the wake of Snowden's disclosures. The Leahy bill, even more than the bipartisan bill that passed the House in May of 2014,[312] would redo the balance between the wide collection and narrow use requirements struck by the FISC's authorization of the metadata program. To preclude the bulk collection that had drawn critics' ire, the Leahy bill would prohibit bulk collection and authorize the government to seek a court order requesting data from phone companies and other private entities based on a "specific selection term."[313] If the "specific selection term" language becomes law, courts will have to preserve a delicate balance: vindicating Congress's post-Snowden intent to limit government collection of U.S. persons' call records, while ensuring that the government continues to have access to records that it has previously been able to obtain by subpoena in routine criminal investigations.

The "specific selection term" language in the Leahy bill in essence codifies the use restrictions imposed by the FISC when it limited queries to searches based on identifiers linked to terrorist groups or other foreign powers. The Leahy bill defines "specific selection term" as a term that "specifically identifies a person, account, address, or personal device, or another specific identifier, that is used by the Government to narrowly limit the scope of tangible things sought to the greatest extent reasonably practicable, consistent with the purpose for seeking the tangible things."[314] The Leahy bill cautions that a specific selection term cannot include terms that are unduly broad, such as terms "based on a broad geographic region, including a city, State, zip code, or area code."[315] While the Leahy bill does an admirable job of tightening up criteria for call record information, courts should be wary of interpreting

312. *See* Amendment to USA Freedom Act of 2013, H.R. 3361, 113th Cong. (2014).

313. *See* S. 2685 § 103(a). The transition from government collection to tailored agency access to privately-held data will be challenging. Telecommunications companies are wary of holding this amount of data, and recent cyber intrusions in the private sector raise doubts about the security of such an arrangement. *See Current and Projected National Security Threats to the United States: Hearing Before the Select Comm. on Intelligence*, 108th Cong. 4–5 (2014) (statement of Sen. Rockefeller, Vice Chairman, Select Comm. on Intelligence). The House bill also requires that companies make the data available to the NSA in an accessible format. Ensuring a user-friendly platform for the data will require cooperation between the public and private sectors.

314. *See* S. 2685 § 107(k)(3)(A)(i) (amending 50 U.S.C. § 1861).

315. *See id.* § 107(k)(3)(A)(ii)(I).

the Leahy bill's language in an unduly narrow fashion. In particular, this language should not be used to prohibit the government from seeking information that has been available by an ordinary subpoena in an ordinary criminal case. For example, in certain circumstances the government may believe that an agent of a foreign power, including a terrorist group, has used a computer in a hotel to send e-mails to associates, but has used an account that is not presently known. In *In re Grand Jury Proceedings, Subpoena Duces Tecum*, the court upheld the validity of a subpoena to obtain all Western Union wire transfers at a Kansas City hotel for a two-year period in an investigation of drug trafficking activity.[316] The court did so despite a claim by the hotel that the request would give the government access to the records of many individuals unconnected to the investigation. While the government's request was broad, it was the narrowest request likely to obtain the information the government sought. A narrower response would frustrate the investigation and would therefore not, using the Leahy bill's language, be "consistent with the [government's] purpose for seeking the tangible things."[317] To avoid unduly intruding on innocent individuals' privacy, the Leahy bill, like earlier FISC decisions on section 215, relies on minimization procedures.[318]

B. Institutional Reform and External Constraints

The Leahy bill seeks to promote articulation of privacy interests in the FISC process, as well as greater judicial review of FISC decisions. It authorizes the FISC to appoint an amicus curiae from a pool of five advocates who would advocate for privacy and civil liberties[319] in a case involving a "novel or significant interpretation of law."[320] It also empowers the FISC to certify matters to the FISCR, and allows the FISCR to certify matters to the Supreme Court. These proposed reforms entail a compromise between the position taken by at least one former FISC judge that most institutional reforms would disrupt the FISC's operation[321] and civil liberties advocates' view that a robust institutional presence was needed to keep the NSA honest.[322] These changes sidestep potential Article III and Appointments Clause objections to more

316. 827 F.2d 301, 302–05 (8th Cir. 1987).

317. *See* S. 2685 § 107(k)(3)(A)(i).

318. *See id.* § 104.

319. *See id.* § 401 (adding new subsection (i)(4)(A)(i) to 50 U.S.C. § 103).

320. *See id.* § 401(i)(2)(A).

321. *See* Letter from Hon. John D. Bates, Dir., Admin. Office of the U.S. Courts, to Sen. Patrick Leahy, Chairman, Comm. on the Judiciary, U.S. Senate (Aug. 5, 2014), *available at* http://online.wsj.com/public/resources/documents/Leahyletter.pdf [hereinafter Bates Aug. 2014 Letter].

322. *See* Marty Lederman & Steve Vladeck, *The Constitutionality of a FISA "Special Advocate,"* Just Security (Nov. 4, 2013, 1:34 PM), http://justsecurity.org/2013/11/04/fisa-special-advocate-constitution.

vigorous reform involving an ongoing institutional role for a public advocate. However, these constitutional objections have clear answers. Courts would have deferred to the role the Supreme Court gave to Congress in the *Keith* case as the democratic arbiter of competing concerns in the national security surveillance domain. Moreover, as a policy matter, the combination of amici curiae and certification relied on in the Leahy bill may not increase adversarial litigation or judicial review of FISC decisions as much as the bill drafters may have hoped. In this sense, the compromise could have been more far-reaching.

Under the Senate bill, the FISC can readily decline to appoint amicus curiae to advocate for privacy and civil liberties, as long as the court "issues a written finding that such appointment is not appropriate."[323] That condition leaves a great deal of discretion with the FISC. Since the FISC did not seek to name amicus curiae before Snowden and at least one former FISC judge spoke out against the proposed change,[324] there is some reason to doubt that the FISC will pivot to enthusiastic support of amici.

1. The Policy Case for a Public Advocate

A more institutionalized public voice at the FISC would be even more valuable than reliance on amici curiae for two reasons.[325] First, a public advocate would enhance the reasoning in FISC decisions. Although the FISC was correct in extending a measure of deference to the executive on the contours of the section 215 relevance standard in place at the time of Snowden's disclosures, the FISC's reasoning left much to be desired. The 2006 FISC opinion, in particular, is truncated and conclusory, offering virtually no analysis.[326] The absence of analysis is problematic. The deliberation that Hamilton extolled in Federalist No. 78 as judicial review's hallmark requires statements of reasons.[327] The statement of reasons sends a useful signal to audiences for the judge's

323. *See* S. 2685 § 401(i)(2)(A).

324. *See* Bates Aug. 2014 Letter, *supra* note 321.

325. *See* Lederman & Vladeck, *supra* note 322.

326. *See In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Name Redacted by Court], No. BR 06-05, 2006 WL 7137486 (FISA Ct. May 24, 2006).

327. Hamilton famously observed that the judiciary has "neither force nor will, but merely judgment." THE FEDERALIST No. 78, *supra* note 12, at 465 (Alexander Hamilton). What distinguishes judgment from force and will is the importance of weighing arguments and giving reasons for accepting or rejecting those arguments. An elaboration of reasons is also the best way to ensure that a decision will not be "arbitrary." *Id.* at 471. Hamilton observed that courts avoid arbitrary decisions because they are bound by precedents, whose "very considerable bulk . . . must demand long and laborious study." *Id.* That bulk, which to be sure has only grown since Hamilton's day, has not accrued from the mere recitation of results, but from the exploration of reasons that drive each outcome. *Cf.* Leib et al., *supra* note 21, at 739 (observing "that judges should be forthright in their opinion writing, explaining honestly why they are deciding as they are.").

decision, conveying the judge's seriousness and ongoing vigilance. In contrast, especially in the secret loop of the pre-Snowden metadata program, a conclusory approval may send a signal to those who have sought judicial authorization that they have more license than the court actually intends. This dynamic may have played a role in the compliance issues that the FISC was forced to deal with in 2009.

The presence of a public advocate would prod the FISC to provide reasons for its decisions. The advocate would receive all government requests. It would be empowered to intervene when it believed that a matter raised novel legal issues, or when it certified to the FISC that there was a reasonable possibility (ten percent or greater) that the government's request failed to meet the statutory standard. The public advocate would present the best legal and factual arguments against the government. The court would then have to weigh the arguments, and explain why it selected one side. The entire process also signals to the government that compliance is a serious matter.

Second, the seriousness imposed by a public advocate would compensate for an even bigger blind spot in the current process: the barely adequate disclosure that the government has provided to Congress. The "rogue robot" explanation for noncompliance furnished by the Justice Department in its December 2009 letter did not supply the comprehensive self-appraisal that Congress has a right to expect.[328] While the Leahy bill provides for more transparency, the cabined deliberation characteristic of Title 50 oversight may not prove sufficiently robust over the long haul. The work of the PCLOB, while exceptionally valuable, may also fail to completely close the gap. An institutional advocate at the FISC would supplement legislative oversight, hedging against future deficits in disclosure to Congress.

The FISC has asserted that an institutionalized advocate would make section 215 authorizations too cumbersome.[329] That risk is real, but manageable. The Leahy bill includes a provision permitting the government to request information on an emergency basis without court

---

328. Weich, *supra* note 38, at 4.

329. *See* Letter from Hon. John D. Bates, Dir., Admin. Office of the U.S. Courts, to Sen. Dianne Feinstein, Chairman, U.S. Senate Select Comm. on Intelligence 2 (Jan. 13, 2014), *available at* http://www.lawfareblog.com/wp-content/uploads/2014/01/1-13-2014-Ltr-to-DFeinstein-re-FISA.pdf; COMMENTS OF THE JUDICIARY ON PROPOSALS REGARDING THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 3–4 (Jan. 10, 2014), *available at* http://www.lawfareblog.com/wp-content/uploads/2014/01/1-10-2014-Enclosure-re-FISA.pdf; *see also* Steve Vladeck, *Judge Bates and a FISA "Special Advocate,"* LAWFARE (Feb. 4, 2014, 9:24 AM), http://www.lawfareblog.com/2014/02/judge-bates-and-a-fisa-special-advocate (arguing that FISC criticism of the special advocate proposal is unfounded because the advocate would only participate in cases involving substantial legal issues and would therefore not clog up routine functioning of court; arguing further that, "even the finest jurists can occasionally benefit from exposure to . . . arguments that they might not have known to ask for and/or affirmatively seek out.").

approval,[330] which the FISC also permitted pursuant to a request after President Obama's January 2014 speech. Over time, an advocate should fit efficiently into FISC proceedings, minimizing delay. An advocate would not appear in the great bulk of FISC cases, but only in those that raise important legal issues, or where the public advocate certified to the FISC that a nonfrivolous factual question had surfaced. In those cases, the familiar analogy to the *ex parte* nature of warrant requests breaks down. In the section 215 context, legal issues have arisen precisely because the government does not have to make the showing of particularized probable cause that it must make to obtain a warrant. The mere process of obtaining a warrant in an ordinary criminal case eliminates the issues that have proven most controversial under section 215. In addition, if a judge issues a warrant in an ordinary criminal case that raises substantial legal issues, that decision will be subject to review at a criminal trial, when the defendant moves to suppress the evidence obtained pursuant to the warrant. In contrast, review of FISC decisions is rare.[331]

Finally, the prophylactic effect of a public advocate would make up for any modest inconvenience. After all, an agency that does not address compliance with the requisite diligence ultimately causes far greater inefficiency, as the FISC discovered when it placed the NSA on a stern remedial regime in 2009. If the presence of an advocate deters another compliance meltdown like the one the FISC addressed in 2009, this innovation will be well worth any modest inefficiencies that ensue.

2. The Legal Case for a Public Advocate

The Leahy bill did not create an institutionalized public advocate. Instead, it granted authority to the FISC to request participation by an amicus curiae on legal issues. That more modest approach was the product of a political compromise with the White House, and perhaps of concerns about how a more robust approach would square with constitutional requirements. Those constitutional questions stem from Article III's requirement that tribunals exercising the "judicial power" of the United States adjudicate only "cases or controversies" and from the Appointments Clause's protection of the President's power to remove inferior officers. I address these issues in turn.

---

330. *See* USA FREEDOM Act of 2014, S. 2685, 113th Cong. § 102 (introduced July 30, 2014).

331. The Foreign Intelligence Surveillance Court of Review has convened only a handful of times. For one such occasion, see *In re* Sealed Case, 310 F.3d 717, 734–36 (FISA Ct. Rev. 2002) (upholding provision of USA Patriot Act that permitted use of evidence obtained through FISA warrant in ordinary criminal case when protection of national security or acquisition of foreign intelligence information was "significant," as opposed to "primary," reason for FISA warrant).

a. The Public Advocate and Article III

Article III's case or controversy requirement ensures that federal courts only hear matters with the concrete adverseness necessary to promote the resolution of live factual or legal disputes.[332] Federal courts do not provide advisory opinions on abstract matters of policy. To steer clear of such matters, which are the province of the other branches, the Supreme Court has interpreted Article III to require that each party to a dispute demonstrate an injury in fact that is more concrete than the generalized injury suffered by the public because of policies with which it disagrees.[333]

Choosing to go the amicus curiae and certification route addressed most of the Article III concerns that a public advocate would engender. An amicus curiae is not a party to litigation. An amicus cannot initiate or agree to settle a lawsuit, and cannot appeal a decision that rejects the position taken by the amicus. An amicus is simply a friend of the court, who participates in litigation at the court's request to provide the court with helpful information. As a non-party, an amicus is not subject to Article III's case or controversy requirement. That non-party status, however, also limits the advantages amicus curiae can offer in opening up a process such as FISC proceedings. As a creature of the court, an amicus can only play a role when the court chooses to authorize the amicus's participation. As we have seen, it is far from clear that the Leahy bill's provisions will permit the participation that the bill's drafters may have viewed as optimal.

i. Certification and Its Discontents

The Leahy bill's insightful drafters sought to anticipate this concern by supplementing provision for amici curiae with a provision for the certification of novel legal issues to the FISCR and to the Supreme Court. Certification also does not involve Article III problems.[334] However, certification has also triggered sufficient resistance from the Supreme Court on prudential grounds.[335] Certification's heyday occurred over a century ago. The prospects for reviving it in the FISC context are as limited as the prospects for making floppy drives a mainstay of 21st century word processing or re-enshrining the VCR as the principal mode for recording visual media.

---

332. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 559–60 (1992).

333. *Id.* at 560.

334. *See* Steve Vladeck, *Article III, Appellate Review, and the Leahy Bill: A Response to Orin Kerr*, LAWFARE (July 31, 2014, 10:54 AM) http://www.lawfareblog.com/2014/07/article-iii-appellate-review-and-the-leahy-bill-a-response-to-orin-kerr.

335. *See infra* notes 320–21 and accompanying text.

Before demonstrating that certification does not adequately address the problem that FISC decisions are unreviewable, it is useful to demonstrate that certification does not present problems under Article III. Certification involves a lower court requesting that a higher court resolve a purely legal issue[336] in a case that already meets Article III requirements. In a case initiated by a party alleging an injury in fact, certification of a legal question to a higher court can resolve legal questions expeditiously or avoid conflicting results in disparate forums, such as the various federal circuit courts of appeals.[337] Certification has a long historical pedigree: through much of the nineteenth century, certification was the approved route for bringing many matters to the Supreme Court, including criminal appeals.[338] Today, certification in the federal system largely involves federal courts, hearing cases based on diversity of citizenship, seeking guidance on state law from a state's highest court.[339] Because certification is a device used by courts to seek guidance in matters that already meet Article III's test, its use in the FISC process prompts no questions beyond those raised by FISC adjudication itself. Those questions, while legitimate, have persuasive answers.

However, the absence of convincing Article III objections to certification of FISC decisions does not mean that certification will provide the enhanced review that the Leahy bill's sponsors seek. At the Supreme Court level, at least, certification has fallen into severe disuse.[340] That reticence stems from prudential doctrines and evolving

---

336. *See* United States v. Union Pac. R.R. Co., 168 U.S. 505, 512 (1897); *cf.* Chicago, Burlington & Quincy R.R. Co. v. Williams, 214 U.S. 492, 496 (1909) (Holmes, J., dissenting) (arguing that the Court should have decided the certified question, as it was issue of "pure law" instead of a mixed question of law and fact).

337. *See* United States v. Seale, 558 U.S. 985, 986 (2009) (Stevens, J., dissenting from dismissal of certification) (arguing that certification can "expedite . . . litigation" and "serve the interests . . . of legal clarity . . . prosecutorial economy . . . and 'the proper administration . . . of judicial business.'"); *compare* Amanda L. Tyler, *Setting the Supreme Court's Agenda: Is There a Place for Certification?*, 78 GEO. WASH. L. REV. 1310, 1322–23 (2010) (discussing virtues of certification), *with* Hon. Bruce M. Selya, *Certified Madness: Ask a Silly Question . . .* , 29 SUFFOLK U. L. REV. 677, 689 (1995) (arguing that certification often produces inefficient litigation, particularly when the record in a case is "insufficiently developed to permit a dispositive answer[]" on the relevant question of law).

338. Tyler, *supra* note 337, at 1323.

339. *See, e.g.*, *In re* Thelen LLP, No. 12-4138, 2014 WL 2931526, at *1–2 (Ct. App. July 1, 2014) (based on certification from United States Court of Appeals for the Second Circuit, determining that hourly fee matters that originated with a now dissolved law firm are not property of the dissolved law firm, and that transfer of those matters to former partners in that firm now working at other firms is not a fraudulent transfer under New York law).

340. *See Seale*, 558 U.S. at 986 (Stevens, J., dissenting) (noting that at the Supreme Court, "[t]he certification process has all but disappeared in recent decades."). The Supreme Court last accepted a case on certification in 1981. The Court disposed of that certification with a ministerial step that suggested no appetite for continued engagement. *See* Iran Nat'l Airlines Corp. v. Marschalk Co., 453 U.S. 919, 919–20 (1981) (in litigation concerning claims against Iran, referring certifying circuit court to

views of court management.[341] At least one distinguished federal appellate judge, who coincidentally later served on the FISCR, has also suggested that certification is often unwise because isolating purely legal questions is not as easy as it sounds.[342] While academics may teach law from casebooks, practicing lawyers and judges know that the holdings memorialized in casebooks grow out of full records. Deciding a legal question without the benefit of that complete record may lead to a decision that lacks grounding in the practical dimensions of commercial, political, or administrative life.[343]

Mindful of these concerns, both the FISCR and the Supreme Court may well resist hearing FISC certifications on the merits. Separating factual issues from purely legal points will be difficult, since so much turns on the continually changing nature of communications.[344] Because of the pace of technological change, even a record compiled a year before an appellate decision may be obsolete. Deciding a case without any record, as certification requires, would be an exercise in rank speculation. Other questions mix law and fact from the outset. As an example, consider the question of whether a "specific selection term" could be a particular hotel server, when the intelligence agency believes that a terrorist has been a guest at the hotel but may be using a previously unknown e-mail account. That question could turn on factual matters, such as the NSA's capacity to retrieve the information through other, less restrictive means. As a mixed question of law and fact, this issue would be unsuited for certification.[345] In short, although the Leahy bill's reliance on certification signals that Congress wants more review of FISC decisions, it is far from clear that certification will achieve that goal.

---

the Supreme Court's decision upholding Iranian claims settlement by the President in Dames & Moore v. Regan, 453 U.S. 654 (1981)).

341. *See* Wisniewski v. United States, 353 U.S. 901, 902 (1957) (per curiam) (dismissing certification to the Supreme Court to resolve splits among different panels of the same circuit on the grounds that the circuit court could promote uniformity by hearing the issue en banc); *cf.* Edward A. Hartnett, *Questioning Certiorari: Some Reflections Seventy-Five Years After the Judges' Bill*, 100 COLUM. L. REV. 1643, 1711 (2000) (discussing reasons for certification's decline); Tyler, *supra* note 337, 1322–23 (same).

342. *See* Hartnett, *supra* note 341, at 1711.

343. *See* Selya, *supra* note 337, at 689 (suggesting that a prudent court will virtually always find a full record useful to making an informed decision).

344. *See* Riley v. California, 134 S. Ct. 2473, 2497–98 (2014) (citing the changing nature of communications in a ruling barring the incidental digital search of cell phones pursuant to the arrest of a suspect).

345. The FISC might transform this into a purely legal question by determining that no narrower means would suffice to retrieve the information. Those findings, however, would effectively determine the case, leaving the Supreme Court with little or nothing to decide.

ii. Warrants, Article III, and the Lessons of History

The uncertain benefits of amici curiae and certification stand in contrast with the more vigorous debate that a true public advocate would promote at the FISC. This more robust institutional reform would not present irremediable legal problems under Article III or the Appointments Clause. To see why, we need to consider the history of warrant applications and the deference that the Supreme Court signaled in *Keith* was owed to Congress in establishing procedures for national security surveillance.

In considering the Article III question, it is best to start with the opinion by the Office of Legal Counsel ("OLC") of the Justice Department that Congress relied on in drafting FISA in 1978.[346] The OLC opinion is generally viewed as a definitive statement of law within the executive branch, with some precedential effect on subsequent executive branch action. In addition, courts, in the nearly four decades since FISA's enactment, have ruled in a fashion that is consistent with the OLC memorandum.[347] While the Supreme Court has not yet weighed in, the unbroken practice of courts in a matter weighted with national security concerns counsels caution in dislodging settled understandings.

The OLC opinion stressed that traditional warrants did not present Article III problems.[348] According to the OLC, warrant applications were "cases and controversies" within the meaning of Article III because they involved two parties with divergent interests: the government, which was seeking authority to conduct surveillance, and the target of the surveillance, who presumably wished to avoid the harm of being monitored. As a court that opined early on regarding FISA's consistency with Article III found, neither traditional warrants nor FISA involved "a desire for an abstract declaration of law."[349] Moreover, the mere fact that an application is made *ex parte*, by only one side, does not present Article III problems.[350] As the Supreme Court said in *Pope v. United States*, when a party goes to court to seek enforcement of a legal right, the "uncontested" nature of the claim does not affect its classification as

346. *See* Memorandum from John M. Harmon, Assistant Att'y Gen., Office of Legal Counsel, to Hon. Edward P. Boland, Chairman, House Permanent Select Comm. on Intelligence (Apr. 18, 1978), *in Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence*, 95th Cong. 26, 31 (1978) [hereinafter Subcomm. Hearings].

347. *See, e.g.*, United States v. Megahey, 553 F. Supp. 1180 (E.D.N.Y. 1982).

348. Subcomm. Hearings, *supra* note 346, at 28.

349. *Megahey*, 553 F. Supp. at 1196 (citing *In re* Summers, 325 U.S. 561, 567 (1945)).

350. *Id.*; Subcomm. Hearings, *supra* note 346, at 28; Pope v. United States, 323 U.S. 1, 11 (1944); *cf.* Stump v. Sparkman, 435 U.S. 349, 357–58 (1978) (in upholding judicial immunity regarding *ex parte* sterilization, the Court stated that nothing in state law prohibited the exercise of jurisdiction over an *ex parte* order).

a case or controversy.[351] A dispute satisfies the case or controversy test when one party seeks to establish a sufficiently specific legal claim or position.[352] The crucial issue is whether a party *could* assert her rights, not whether a party is actually asserting her rights in this particular phase of litigation.

The history provided in Justice Powell's opinion for the Court in *Keith* fits this view of the interaction of warrant applications and Article III.[353] The Fourth Amendment crystallized leading English jurists' practice of insisting on an approval of warrants by a neutral magistrate[354] who was "independent of the police and prosecution."[355] Justice Powell cited Lord Mansfield's pathbreaking opinion in *Leach v. Three of the King's Messengers*[356] on the need for a neutral magistrate. The Framers were familiar with this line of cases.[357] Moreover, the Framers clearly believed that the Constitution, even prior to the addition of the Bill of Rights, preserved the ancient, unwritten "rights of Englishmen" that the leaders of the American Revolution claimed had been trampled by King George III and the British Parliament, including the right to neutral checks on unbridled law enforcement.[358] It would be inconsistent with the Framers' intent to interpret Article III as barring federal judges from this checking role. While the Court has held that even lowly court clerks can issue warrants,[359] surely independence is best ensured by providing for the issuance of warrants by Article III judges protected by lifetime tenure. Justice Powell's opinion for the Court in *Keith* never mentioned any Article III problems with the "traditional Fourth Amendment requirement [that] . . . a neutral and detached magistrate" approve

---

351. *Pope*, 323 U.S. at 11.

352. Subcomm. Hearings, *supra* note 346, at 28; *In re* Penn Cent. Transp. Co., 384 F. Supp. 895, 911 (Spec. Ct. 1974).

353. *Keith*, 407 U.S. 297, 316 (1972).

354. *Id.*

355. *See* Shadwick v. City of Tampa, 407 U.S. 345, 347–49 (1972).

356. (1765) 97 Eng. Rep. 1075 (K.B.) 1088 (noting, in the opinion by Lord Mansfield, that, "[t]he magistrate ought to judge" the scope of an arrest warrant, and "give certain directions to the officer[]" executing the warrant, rather than relying on that officer's discretion) (cited in *Keith*, 407 U.S. at 316).

357. David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739, 1799 (2000) (noting that broad warrants executed in the 1760s on English dissidents were invalidated on a range of grounds by English courts, including the absence of prior approval by a neutral magistrate, and that this judicial safeguard was important to the Framers). *But see id.* at 1800 (noting that English precedents from the Revolutionary era focused on several factors that resist refinement into a single test).

358. *Cf.* Steven G. Calabresi et al., *State Bills of Rights in 1787 and 1791: What Individual Rights Are Really Deeply Rooted in American History and Tradition?*, 85 S. CALIF. L. REV. 1451, 1456–57 (2012) (noting rhetoric during the Revolutionary era about the rights of Englishmen, while observing that such rhetoric entailed a range of conceptions that varied among states). The proposition in the text would still stand if rhetoric about the rights of Englishmen served as a proxy for an emerging American consensus that expanded on the English tradition. *See id.* at 1546.

359. *See Shadwick*, 407 U.S. at 348.

search warrants.[360] Indeed, Justice Powell referred to the need for a "prior judicial judgment,"[361] invoking the language of judicial power used in Article III. It seems reasonable, therefore, to read Article III in tandem with the practice of obtaining a warrant from a neutral magistrate that was codified by the Fourth Amendment.

Although the executive receives more latitude in surveillance of non-U.S. persons located abroad and the FAA does not require individual warrants, the conflict with Article III is not materially greater in the foreign surveillance context. Limiting the executive to targeting non-U.S. persons located abroad entails safeguards tailored to overseas surveillance. Congress's judgment on the framework necessary to accomplish these goals is worthy of deference. Congress is certainly not required to assume a passive role, trusting that the government will not use the foreign intelligence rubric to spy on U.S. persons. As Chief Justice Roberts noted in his opinion for the Court in *Riley*, trusting solely in internal government "protocols" is a poor substitute for independent safeguards.[362] Moreover, even when the executive can proceed without a warrant, as in a search that is a bona fide effort to recover foreign intelligence information, the courts can still assess the reasonableness of the search under the Fourth Amendment.[363] Congress can play a role in codifying basic standards of reasonableness in such searches. It would be ironic if the courts, in the name of preserving the judicial role under Article III, were to diminish the safeguards that Congress put in place to preserve an independent judicial check on executive overreaching.

Justice Powell's opinion in *Keith* seemed to echo this concern. Justice Powell suggested that a request for court approval of warrants in domestic national security cases could go to a "specially designated court"[364] and that such approval may be governed "in accordance with such reasonable standards as the Congress may prescribe."[365] This deference would support a robust public advocate with an ongoing role in FISC proceedings and the capacity to appeal FISC rulings that the advocate deemed to be insufficiently protective of privacy and civil liberties.

If one needed a more concrete basis for requiring participation in FISC proceedings by a public advocate, one could also invoke the "next friend" doctrine. Courts have repeatedly recognized that a "next friend" may invoke the rights of an absent party who meets the Article III

360. *Keith*, 407 U.S. at 317 n.18.
361. *Id.* at 317.
362. Riley v. California, 134 S. Ct. 2473, 2491 (2014).
363. United States v. Butenko, 494 F.2d 593, 604 (3d Cir. 1974) (en banc).
364. *Keith*, 407 U.S. at 323.
365. *Id.* at 324.

requirement of an injury in fact.[366] Here, the target of surveillance—the real party in interest—surely has an injury in fact, since being subject to unwanted surveillance is a substantial government intrusion. The Supreme Court has recognized that the "inaccessibility" of the real party in interest is a factor in assessing the propriety of next friend status.[367] In responding to *Keith*'s invitation, Congress could establish a public advocate as an institutional next friend for surveillance targets, who cannot be present because notice to them would undermine the purpose of surveillance. As a practical matter, surveillance targets are inaccessible to the magistrate deciding a warrant request because targets do not receive notice. In this sense, targets resemble an individual who is being held incommunicado, where courts have indicated that appointment of a next friend is appropriate.[368] In both cases, the real party in interest cannot make its wishes known, and a next friend can act on the reasonable presumption that the real party in interest would prefer to be free from state coercion or intrusion. Appealing from an adverse judgment would simply be another function fulfilled by a next friend representing the real party in interest.

If a congressional framework establishing a public advocate as a next friend would be entitled to deference, the modest steps in the Leahy bill merit even greater solicitude. The Leahy bill's requirement that the FISC explain in writing why it has failed to appoint amicus curiae is not problematic as an interference in matters reserved to courts. Congress has, on occasion, required courts to produce writings in connection with certain relief. For example, a circuit justice or judge must issue a certificate of appealability to permit appeal by criminal defendants of final orders denying habeas relief.[369] While rules on habeas appeals arguably merely govern the substantive rights of the parties, with the issuance of the certificate being ancillary to those rights, that distinction seems unduly rigid. It is true that appointment of amicus curiae has traditionally been viewed as the court's prerogative. However, Congress can modify other powers that courts have traditionally exercised, such as the power to grant injunctive relief.[370] The writing required by Congress here is a far more modest limit on judicial discretion.

---

366. *See* Al-Aulaqi v. Obama, 727 F. Supp. 2d 1, 16–17 (D.D.C. 2010) (in the course of holding that the father of an alleged overseas target of U.S. government-targeted killing lacked standing to be a next friend, the court observed that next friend standing required that the real party in interest meet the injury in fact requirement of Article III).

367. Whitmore v. Arkansas, 495 U.S. 149, 163 (1990).

368. Coalition of Clergy v. Bush, 310 F.3d 1153, 1159–60 (9th Cir. 2002).

369. *See* 28 U.S.C. § 2253 (2006).

370. *See* Winter v. Natural Res. Def. Council, 555 U.S. 7, 24 (2008); Jared A. Goldstein, *Equitable Balancing in the Age of Statutes*, 96 VA. L. REV. 485 (2010).

b. The Public Advocate and the Appointments Clause

The final problem with a robust public advocate centers on the Appointments Clause.[371] The Appointments Clause requires that any principal officer, such as a cabinet official or ambassador, be appointed by the President and confirmed by the Senate, while inferior officers may be appointed by the President, the courts, or other executive branch officials. To ensure democratic accountability, a principal officer must be removable by the President directly, while Congress can provide that an inferior officer is removable only by a principal officer and only for good cause.[372] To ensure maximum independence for a public advocate, appointment by the courts as an inferior officer would be preferable. Some argue, however, that a public advocate cannot meet the standard for inferior officer status. These arguments are misplaced.

The classic case is *Morrison v. Olson*, in which the Court held that the independent counsel established by Congress in the wake of Watergate was an inferior officer whose appointment by the courts and insulation from direct removal by the President therefore passed constitutional muster.[373] Justifying its decision, the Court noted that Congress enacted the independent counsel statute because of concern about "conflicts of interest" created when the executive branch is permitted to investigate itself.[374] To ease these conflicts, Congress lodged appointing authority in the judiciary.[375] However, the Court recognized that granting the judiciary appointment authority would be unconstitutional if that authority appeared to undermine the judicial role or impose responsibilities on the courts that were "incongruous" in light of that role. The Court did not regard the courts' appointment of an independent counsel as "incongruous," even though the independent counsel served as a prosecutor who appeared before the courts in criminal litigation and took legal positions that the courts were required to evaluate.[376] Although some have argued that subsequent decisions have diluted *Morrison*'s force,[377] those decisions do not deal with checks on national security surveillance in the wake of Snowden's disclosures.

---

371. U.S. CONST. art. II, § 2, cl. 2.

372. Free Enter. Fund v. Pub. Co. Accounting Oversight Bd., 561 U.S. 477, 490–91 (2010).

373. 487 U.S. 654, 671 (1988).

374. *Id.* at 677.

375. *Id.*

376. *Id.*

377. *See* NOLAN ET AL., *supra* note 41 (citing *Pub. Co. Accounting Oversight Bd.*, 561 U.S. at 490–91). *See generally* Patricia L. Bellia, PCAOB *and the Persistence of the Removal Puzzle*, 80 GEO. WASH. L. REV. 1371, 1389–1412 (2012) (discussing history and future prospects). *But see* Steven G. Calabresi & Kevin H. Rhodes, *The Structural Constitution: Unitary Executive, Plural Judiciary*, 105 HARV. L. REV. 1153 (1992) (arguing that the Constitution bars limits on the President's power to remove executive branch officials).

In establishing a public advocate, Congress would be acting not only on *Keith*'s invitation, but also on the premise that the system in place at the time of Snowden's disclosures did not provide sufficient independence from the government's positions. A public advocate would supply a robust institutional check analogous to the independent counsel's service when conflicts of interest disabled regularly appointed federal prosecutors. Although the public advocate's role would be ongoing, not the limited and exceptional service provided by the independent counsel, that distinction is unimportant. The public advocate's function in promoting independent assessment of the government's position is central to her inferior officer status. Deferring to Congress's determination of the urgency of promoting independent, adversarial adjudication of national security surveillance after Snowden is of a piece with deference to Congress's fix for the problem of the executive investigating itself in the wake of Watergate.

C. "About" Collection Under Section 702

The dynamic conception also illuminates another controversial issue: NSA's collection, under section 702 of the FAA, of the content of communications "about" suspected terrorists and others who can provide foreign intelligence information. Critics have asserted that this practice, which the FISC approved in 2011, stretches to the breaking point the "target" language in section 702.[378] While the acquisition of information under section 702 is not bulk collection, it raises significant issues, including whether the NSA should be able to query section 702 data with U.S. person identifiers—a concern addressed in the next Subpart. Ultimately, however, "about" collection is consistent with the NSA's governing statute.

According to critics, a "target" is best understood as a person who either sends or receives communications.[379] That limit on targeting keeps collection within manageable bounds, critics contend. Critics worry about the scope of "about" collection. Suppose, critics have posited, that the NSA defines a communication "about" a given matter as one in which that subject is mentioned one or more times in the communication. Using this working definition, suppose the NSA targeted all communications that mentioned "Al Qaeda" or "Osama bin Laden." Many people around the world, including journalists, academics, and ordinary citizens, use such terms in e-mails or phone conversations, without possessing any links to terrorism or other activities of foreign intelligence import. For critics, defining "target" in section 702 to include this wide set of communications about matters of foreign intelligence interest echoes the

378. *See, e.g.*, Donohue, *supra* note 8 (manuscript at 58).
379. *See id.*

broad definition of relevance that the FISC relied on to justify the metadata program under section 215.[380]

Even if one accepts the critics' point about FISC interpretation of section 215, the government is on firmer footing here. Collection of communications "about" a target is hardly novel under laws dealing with foreign intelligence information. Although much targeting aims to collect information to or from a particular individual, targeting can encompass more. Explaining the meaning of "target" in the original FISA legislation in 1978, the House Permanent Select Committee on Intelligence ("HPSCI") stated that "the target of . . . surveillance is the individual or entity *about whom* or from whom information is sought."[381] As if replying to those who might view the term, "target," in more restrictive terms, the House Report advised that, "[i]n most cases this would be the person or entity at whom the surveillance is physically directed . . . but this is not necessarily so."[382] The Committee evidently believed that, in the realm of foreign intelligence collection, the government needed further leeway.

This is unsurprising if one views surveillance abroad as a fiduciary activity designed to bridge gaps in knowledge about security risks. That knowledge is necessarily imperfect.[383] Gaps in knowledge can be dangerous, leading to a failure to connect the dots. To guard against this failure, a diligent intelligence official will want to know as much as possible about the associates and capabilities of a foreign subject. Limiting intelligence collection to communications dutifully exchanged between a subject and his known associates hinders this objective. The diligent analyst will be even more interested in previously *unknown* associates or activities of the subject. Extending collection to communications "about" the subject will ferret out this information.

In "about" collection, tailored criteria for defining the subjects of collection are vital, both legally and functionally. Over-inclusive criteria may be arbitrary, unduly intrusive on innocent parties, or simply counterproductive. For example, collecting messages that include the words "Al Qaeda" or "Osama bin Laden" will result in a flood of irrelevant information useless to the analyst. To be usable, such a trough of information would have to be subjected to additional queries, all of which take time and effort. While some analysts, left to their own devices, might take this approach, both U.S. domestic law and international law require a more targeted strategy.[384] That is why the NSA uses precise or "strong" selectors, such as e-mail addresses or

380. *Id.*
381. *See* H.R. REP. No. 95-1283, pt. 2, at 73 (1978) (emphasis added).
382. *Id.*
383. Holder v. Humanitarian Law Project, 561 U.S. 1, 32–39 (2010).
384. *See* Margulies, *supra* note 85, at 2159–60.

phone numbers.[385] Because of the small set of people with knowledge of the e-mail address or phone number of a subject of foreign intelligence interest, strong selectors weed out innocent, casual, or inadvertent communications. Selectors with this degree of precision guard against indiscriminate data collection.

Critics counter that the "about" collection enhances the risk that the NSA will collect purely domestic communications that are outside section 702's scope.[386] The NSA collects section 702 data in two forms: through specific requests to ISPs and telecommunications companies (the PRISM program) and through scanning the contents of buffers for international Internet transmissions that comprise part of the Internet's backbone (the Upstream program). "About" collection occurs only in the Upstream program.[387] Upstream scanning raises the risk of acquiring domestic communications that the government could otherwise obtain with a traditional warrant.

The risk of acquiring purely domestic communications stems from the architecture of the Internet and the limits of the NSA's own technology. First, consider the problems rooted in Internet architecture. Internet communications occur in packets.[388] Devices, such as routers, that are programmed to manage packet transmission will take the most efficient path available to a recipient. Sometimes a router will discover that the most efficient path for a particular packet of domestic communications lies through equipment typically used by foreign nationals. If so, the router will take this path. A U.S. Internet user may also change settings in a way that will increase the likelihood that some or all of the user's communications will run through such equipment. When the government conducts a scan of the portion of the Internet backbone typically used for the transmission of international communications, it uses Internet protocol (IP) filters to focus its scan on communications in which either the sender or recipient is reasonably believed to be located outside the United States.[389] The use of IP filters is one aspect of the government's efforts to exercise due diligence in avoiding collection of wholly domestic communications.[390] However, no technology is perfect, and the nature of the Internet architecture means that any program that scans international communications at the Internet

385. PCLOB SECTION 702 REPORT, *supra* note 31, at 32–33.

386. *See, e.g.*, Donohue, *supra* note 8 (manuscript at 58).

387. NAT'L SEC. AGENCY, NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT: NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702 5 (2014) [hereinafter NSA PRIVACY REPORT].

388. *See In re* Government's Ex Parte Submission of Reauthorization Certification for 702 Program, No. [Redacted], 2011 WL 10945618, at *9–11 (FISA Ct. Oct. 3, 2011) (Bates, J.); PCLOB SECTION 702 REPORT, *supra* note 31, at 38.

389. PCLOB SECTION 702 REPORT, *supra* note 31, at 38.

390. *Id.*

backbone stage will acquire some communications in which both sender and recipient are either U.S. persons or individuals located in the United States.

In the Upstream program, the interaction of Internet architecture and limited collection technology creates an additional risk that the NSA will acquire purely domestic communications. Because the Upstream collection occurs at the Internet backbone level, the NSA acquires data in the form of communications "transactions."[391] A transaction is any set of data traversing the Internet that a device combines to facilitate transmission. Internet transactions come in two varieties. The first is a single communication, such as an e-mail message sent from one server to another.[392] The second transaction, called a multiple communications transaction ("MCT"), contains many discrete communications.[393] For example, at the Internet backbone level at which the NSA scans for Upstream collection, e-mails are typically "bundled together within a single Internet transmission."[394]

As of June 2014, the NSA has not been able to design a filter that acquires only those discrete e-mails in an MCT that mention a particular subject of interest.[395] To collect the e-mail that meets its targeting criteria, the NSA also must collect entire MCTs, analogous to pages of personal e-mails. As with anyone's e-mail, an entire page will include some twenty or thirty messages, typically on disparate subjects with different senders. Some MCTs include messages sent between persons located in the United States—that is, purely domestic communications.[396]

A combination of external and internal constraints addresses this problem. The FISC, in its review of the government's section 702 certifications, reviews not only the four corners of the written certification but also the implementation of government measures to minimize use of U.S. person data.[397] Congressional committees exercising oversight can also inquire about those internal constraints, which are extensive and methodical. For example, whenever the NSA acquires an MCT that may contain discrete communications between persons reasonably believed to be located in the United States, the agency will segregate that transaction in an "access-controlled repository."[398] Access is limited to analysts trained in identifying

391. *See In re Government's Ex Parte Submission*, 2011 WL 10945618, at *10–11; PCLOB SECTION 702 REPORT, *supra* note 31, at 39.

392. PCLOB SECTION 702 REPORT, *supra* note 31, at 39.

393. *Id.*; *see* PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMC'NS TECHS., *supra* note 30, at 141.

394. *Id.* at 141.

395. PCLOB SECTION 702 REPORT, *supra* note 31, at 40.

396. *Id.* at 41.

397. *Id.* at 27.

398. *Id.* at 54.

domestic communications transactions. If that trained analyst determines that the transaction contains a discrete domestic communication, the analyst will destroy the entire transaction upon making that determination.[399]

These constraints are not perfect. As with any procedure, one cannot categorically rule out instances of abuse. However, FISC review and congressional oversight minimize the likelihood of problems. The only other alternative would be to preclude "about" collection. As we have seen, however, legislative history and policy point to continuing this collection mode. Speculation about implementation issues should not trump those arguments, particularly given robust internal and external constraints.

D. Querying Databases for Data Incidentally Collected on U.S. Persons

The third issue that merits discussion is the NSA's practice of using U.S. person identifiers to query certain data collected under section 702. Some critics of the NSA have viewed such queries as "back-door surveillance" of U.S. persons. Here, too, however, a look at the tailored nature of the practices in question eases those concerns, although further independent external constraints would enhance the legitimacy of the program and respond to the critics.

The NSA's authority under the FAA to collect communications where a sender or recipient is a U.S. person (as long as the other person is not) creates a potential problem. In theory, the NSA has the capacity to engage in reverse targeting, framing selectors that it knows would net the communications of U.S. persons while using surveillance on non-U.S. persons as a convenient pretext.[400] This practice is illegal: the statute bars collection "where the purpose of targeting somebody outside the United States is to target somebody in the United States."[401] However, critics have expressed fear that policing that prohibition is difficult. That obstacle to enforcing the bar sets the stage for what critics have called "back-door targeting" of U.S. persons.[402] Resort to back-door targeting would be a serious problem, because the absence of a warrant

399. *Id.*

400. *See* Donohue, *supra* note 8 (manuscript at 158–59).

401. 154 Cong. Rec. S6181 (daily ed. June 26, 2008) (statement of Sen. Rockefeller); 50 U.S.C. § 1881a(b)(2) (2014).

402. That dystopian vision is exactly what led Congress in 2008 to omit the language in the Protect America Act of 2007, the FAA's predecessor, which had permitted collection of content "concerning" foreign intelligence. *See* 154 Cong. Rec. S6471 (daily ed. July 9, 2008) (statement of Sen. Feinstein) (observing that, under the previous statute, "[i]f the NSA wanted to get my communications but did not want to go to the FISA Court, they might try to figure out who I am talking with and collect the content of their calls to get to me.").

requirement under the FAA hinges on one party to a conversation being a non-U.S. person reasonably believed to be located abroad. For intentional collection on U.S. persons, the government should seek a warrant under traditional FISA[403] or Title 18.[404] Permitting intentional collection on a lesser showing undermines constitutional protections for U.S. persons.

The NSA has imposed an internal constraint, which is monitored by the FISC and Congress and makes "reverse targeting" far more difficult. The section 702 program that would create the highest risk of reverse targeting is the Upstream Internet transaction program, since that program inadvertently collects a significant amount of U.S. person data through fleeting shifts in Internet protocols and MCTs. To guard against the risk of reverse targeting, the NSA prohibits the use of U.S. person queries with Upstream Internet transaction data.[405]

In programs other than Upstream, the NSA queries the content of communications with U.S. person identifiers, such as a phone number or e-mail address, when such queries would be "reasonably likely to return foreign intelligence information."[406] Queries may stem from a list of persons already subject to court orders under FISA.[407] In such cases, surveillance is already authorized under an individualized determination. The NSA also requires a layer of internal review before an analyst can conduct a query using a U.S. person identifier: the NSA Office of General Counsel must approve requests that do not entail queries based on a prior FISA court order.[408] At the NSA, queries using U.S. person identifiers have been relatively modest: 198 were approved in 2013.[409]

The CIA can also query content with U.S. person identifiers under a similar standard based on the likelihood of returning foreign intelligence information.[410] A CIA analyst does not need pre-approval from another CIA official, but must document in writing why she believes that a particular query meets the standard.[411] The CIA's queries may involve U.S. persons abroad "engaged in facilitating international terrorism."[412] That description would cover U.S. persons who have gone abroad to fight in Syria or Iraq with groups such as the Islamic State of Iraq and Syria ("ISIS"), which has taken over a significant amount of territory in

403. 50 U.S.C. § 1801 (b)(2) (2006).

404. 18 U.S.C. § 2510-22 (2006).

405. NSA PRIVACY REPORT, *supra* note 387, at 7.

406. NSA Minimization Procedures § 3(b)(6) (2011); NSA PRIVACY REPORT, *supra* note 387, at 7; PCLOB SECTION 702 REPORT, *supra* note 31, at 57.

407. PCLOB SECTION 702 REPORT, *supra* note 31, at 57.

408. *Id.*

409. *Id.*

410. *Id.*

411. *Id.* at 58.

412. *Id.*

those two countries and which the United States has designated as a terrorist group. In 2013, the CIA conducted 1,900 content queries of section 702 data with U.S. person identifiers. That is substantially more queries than the NSA performed, although the number is still low enough to suggest that the CIA's queries have been consistent with the legal standard.

Current legislation does not preclude the government's use of U.S. person identifiers in the circumstances just described. The statute prohibits the government from "intentionally" targeting a person reasonably believed to be located outside the United States when "*the* purpose" of this acquisition of data is the targeting of an individual reasonably believed to be in the United States.[413] The terms "intentionally" and "the purpose" should be construed narrowly. Similarly, the term, "target," should be construed to include the element of intent on the part of the analyst doing the query.

A staple of legal discourse on states of mind is the difference between intent and knowledge; intent (along with purpose) refers to a conscious aim, while knowledge merely means awareness of a fact. Countless statutes reflect this distinction, including those that make criminal responsibility or sentencing contingent on a given state of mind. Congress should be credited with knowing the difference when it enacted section 702. The term, "the purpose," is also contrasted with a broader phrase, like "*a* purpose." Use of the definite article refers to a particular thing, not one of many. Congress was quite familiar with this distinction when it enacted the FAA, since the USA Patriot Act had changed the language in a different FISA provision from "the purpose" to "a significant purpose" to allow greater information sharing between intelligence agencies and federal law enforcement in the wake of the failure to connect the dots of the 9/11 plot.[414]

The definition of "target" includes an element of intent. The dictionary definition of the transitive verb "target" describes the word as an effort "to make a target of" or "to direct or use toward a target."[415] Verbs like "make" and "direct" connote a deliberate goal. The legislative history of the original FISA reinforces this point. As previously noted, the HPSCI, in its report on the original 1978 FISA legislation, stated that "the target . . . is the individual or entity about whom . . . information *is*

413. 50 U.S.C. § 1881a(b)(2) (2014).

414. *See id.* § 1804(a)(6)(B) (2014); *In re* Sealed Case, 310 F.3d 717, 723–32 (FISA Ct. Rev. Sept. 9, 2002). That provision allowed the FISC to authorize a FISA warrant on a showing that gathering foreign intelligence information was "a significant purpose" of the request. It replaced the more demanding test, imposed by earlier courts interpreting the former term, "the purpose," that gathering foreign intelligence information, not criminal investigation, was the government's "primary purpose" in seeking a FISA warrant. *Id.*

415. *See* MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 1278 (11th ed. 2003).

sought."[416] Information or any other commodity that is "sought" is consciously desired by the seeker.[417]

The path to enactment taken by the FAA also meshes with these definitions. During the debate in the House of Representatives on the FAA, Representative Sheila Jackson Lee, Democrat of Texas, offered an amendment that had earlier been stripped from the bill. That amendment required a traditional FISA warrant whenever a "*significant* purpose of an acquisition is to acquire the communications of a specific person reasonably believed to be located in the United States."[418] Representative Jackson Lee's amendment would have expanded the meaning of the term "purpose" by removing the definite article "the" that immediately precedes it, and adding the adjective, "significant," which could apply to one of a number of goals, not a single primary objective. Because of the NSA's mission, it will typically have *some* interest in uncovering the identities of Americans whose identifiers appear in section 702 data. That interest would have run afoul of Representative Jackson Lee's amendment. If the amendment had been adopted, it would have curbed the NSA's ability to collect communications of foreign intelligence interest in which one party was a U.S. person. However, the amendment failed in the House, leaving intact the language in the final legislation. Congress's refusal to include Representative Jackson Lee's amendment in the final bill suggests that Congress did not want to unduly hinder the NSA's collection authority.

Policy factors echo this analysis. Selectors that are effective under section 702 will precisely identify targets of foreign intelligence interest, including foreign terrorist groups or officials in governments that sponsor terrorism. Devising selectors to achieve this goal is section 702's driving purpose. As discussed in the previous Subpart, sloppy selectors that took in U.S. person data would ill serve this objective. Admittedly, in some cases the analyst who frames a precise selector may *know* that such collection will also net data about a U.S. person. However, that factor should not in itself limit collection on a valid non-U.S. target. This prohibition would perpetuate gaps in intelligence, instead of closing them. It would also penalize an analyst for knowing *more* about a non-U.S. subject's contacts, if those contacts happen to include U.S. persons. Encouraging analysts to know *less* impairs efficient collection of data about national security threats.

That said, the government's current criteria for use of U.S. person identifiers on section 702 could benefit from further legislative guidance.

---

416. *See* H.R. REP. NO. 95-1283, pt. 2, at 73 (1978).

417. The term, "sought," is the past participle of the verb, "seek," which *Merriam-Webster's Dictionary* defines as, "to try to discover" or "to try to acquire or gain." To "try" to achieve something also connotes a conscious aim. MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 1124 (11th ed. 2003).

418. 154 CONG. REC. H5740 (daily ed. June 20, 2008) (statement of Rep. Jackson Lee) (emphasis added).

Guidance from Congress could clear up one area of inconsistency within NSA's own criteria, involving the use of identifiers to gather information about threats to life. It could also refine areas where the use of U.S. person identifiers serves foreign intelligence goals, including aggregating information about conduct abroad on behalf of a foreign terrorist organization, participation in a transnational criminal enterprise, and espionage.

Consider first the status of "threats to life" as a basis for framing U.S. person queries of section 702 data. The NSA's own example—hostage situations—does not fit the NSA's stated criteria of a query that is "reasonably likely to return foreign intelligence information."[419] At first blush, this argument about the inconsistency of gathering information about hostage situations with the NSA's criteria for use of U.S. person identifiers may seem counterintuitive. Who, after all, could argue with gathering as much information as possible to deal with such exigencies? In policy terms, the NSA's position may well be the right call. However, it poses tensions with the NSA's own criteria for using U.S. person identifiers.

To see why, consider three common examples of hostage situations. A typical U.S. hostage situation involves a bank robbery gone wrong or an episode of domestic violence, in which a batterer holds an intimate partner or a child hostage after the police arrive. In this situation, foreign involvement is not likely; indeed, it is rare. A query in this case would be largely precautionary in nature, obviating the remote possibility of foreign involvement. Next, consider a hostage situation abroad. Here, the *victim* might be a U.S. person, but it is uncertain whether a section 702 query based on the U.S. victim's discrete identifiers would yield foreign intelligence information, unless the victim had engaged in prior communications with her captors or the captors engaged in communication about the victim. The latter instance (of kidnappers mentioning the victim) is possible, but would only be "likely" if the analyst making the query knew more, such as whether the government's section 702 data included surveillance of the foreign individual or group responsible for the kidnapping. The return of foreign intelligence information would also be likely where a U.S. person takes hostages abroad, but this is exceedingly infrequent. Here, too, knowing more might change the calculus; if a group like ISIS took hostages, it is possible that further information would be available from querying identifiers associated with U.S. persons known to have joined the group. Even here, however, it is not necessarily "likely" that such a query would return foreign intelligence information, since U.S. persons who have joined the group might have no knowledge of the kidnapping. This does

419. NSA PRIVACY REPORT, *supra* note 387, at 7.

not mean that Congress should bar such queries in hostage situations, but it does call attention to the lack of fit between the NSA's current stated criteria and its own examples.

Remedying the problems with NSA's use of U.S. person identifiers is more challenging. Two current proposals—one by Representative Zoe Lofgren of California, which the House of Representatives has approved, and one by Chair David Medine and former D.C. Circuit judge Patricia Wald of the PCLOB—illustrate the difficulties plaguing proposed solutions.

Consider first the amendment to the Department of Defense Appropriations Act offered by Representative Lofgren.[420] The Lofgren Amendment would bar using federal funds "to query a collection of foreign intelligence information acquired under section 702 . . . using a United States person identifier."[421] The only exception in the amendment is for identifiers connected to traditional FISA warrants and other ex ante court orders authorizing surveillance.

The Lofgren Amendment paints with an unduly broad brush. It does not allow queries based on U.S. persons who are involved with hostage situations. Even though this query does not readily fit with the NSA's current criteria, barring it altogether would be counterproductive. In exigent cases, the NSA should have the ability to frame queries that may save lives. The Constitution presents no bar since courts have regularly approved searches under exigent circumstances.[422] Nor does the use of U.S. person queries in hostage situations clash with section 702's bar on targeting U.S. persons, since the queries concern evidence already acquired through the targeting of persons reasonably believed to be outside the United States.[423]

Moreover, the government may well have the need to seek other information regarding U.S. persons that could be included in lawful collection under section 702 and might be difficult to acquire through other means. For example, the government might intercept communications sent or received by an ISIS operative in Syria or Iraq, and might wish to know if the ISIS operative mentioned any U.S. persons who are currently abroad fighting on ISIS's behalf or might wish to go abroad for this purpose. It is true that the government might be able to secure a traditional FISA warrant once it determined that someone had taken concrete steps to join ISIS's fighting force, since that would make that individual an "agent of a foreign power" who could be targeted

420. *See* 160 CONG. REC. H5544 (daily ed. June 19, 2014).

421. *Id.*

422. *See* Riley v. California, 134 S. Ct. 2473, 2494 (2014); Kentucky v. King, 131 S. Ct. 1849, 1856 (2011).

423. *See* United States v. Mohamud, NO. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *26 (D. Ore. June 24, 2014) (holding that the Fourth Amendment does not bar U.S. person queries of section 702 information that has been lawfully acquired).

under the statute.[424] However, in a particular case, such as one in which a U.S. person who had fought with ISIS was about to board a plane to return to the United States, time might be of the essence. In such a case, the government may not have received sufficient notice of that individual's ISIS involvement to allow for the completion of a traditional FISA application. Under these circumstances, it would be appropriate to authorize a query of a section 702 database. The Lofgren Amendment also fails to address this situation.

Another flawed fix is the proposal by Chairman Medine and Judge Wald of the PCLOB. That proposal requires ex ante judicial review of NSA queries to ensure that they are "reasonably likely to return foreign intelligence information."[425] This proposal is superior to the Lofgren Amendment because it has an appropriately deferential substantive standard. Moreover, a larger FISC role is useful.[426] In addition, Medine and Wald outlined an intriguing alternative, entailing FISC appointment of a special master who could review a "representative sample of query results" and make recommendations to the court.[427] The major flaw in the Medine and Wald proposal is its differential standard for the NSA and the FBI. Under the proposal, the test for the FBI, as assessed ex ante by the FISC in all but exigent circumstances, would be whether the U.S. person query is "reasonably likely to return information relevant to an assessment or investigation of a crime."[428] The NSA's test is whether the query is "reasonably likely to return foreign intelligence information."[429] The differing criteria for FBI and NSA queries could hamper intelligence sharing between the two agencies, replicating the failures of the "wall" that existed between agencies prior to September 11.[430]

The better course for Congress would be to offer an itemized, but not exhaustive, list of permissible uses of U.S. person identifiers. Congress could permit U.S. person queries in cases involving pre-existing FISA orders, threats to life, efforts to join international terrorist groups (the ISIS example), and other transnational illegal activity. This list would not categorically bar other uses of U.S. person identifiers, allowing some room for those uses when compelling circumstances arise.

---

424. *See* 50 U.S.C. § 1805(a) (2006).

425. *See* PCLOB SECTION 702 REPORT, *supra* note 31, at 157–58.

426. *See ID.* at 158 (citing *Riley*, 134 S. Ct. at 2491) (observing that the Founders favored independent ex ante review of government searches, and "did not fight a revolution to gain the right to government agency protocols").

427. *Id.* at 157 n.567.

428. *Id.* at 138, 159.

429. NSA PRIVACY REPORT, *supra* note 387, at 7.

430. *See In re* Sealed Case, 310 F.3d 717, 734–36 (FISA Ct. Rev. Sept. 9, 2002) (upholding the statutory change that tore down the wall by permitting the prosecution to use information acquired through a FISA warrant when gathering foreign intelligence information was "significant" but not the "primary" purpose of the warrant).

However, it would frame the substantive discussion in a useful way, and send a signal to the FISC and the executive branch that deliberation on the scope of U.S. person queries was vital.

A set of guidelines like those suggested would also compensate for the broader latitude that the NSA has for incidental collection under section 702. In cases that comprise the basis for the incidental collection doctrine, a federal judge had already issued a warrant based on probable cause to believe that wrongdoing had occurred.[431] That is not the case with section 702, where the FISC merely reviews government targeting procedures.[432] The latitude permitted under section 702 gives the government more room to frame initial searches to ensnare Americans. Critics have surely exaggerated the government's ability to engage in reverse targeting. Evidence that the NSA has engaged in such practices is slim to nonexistent. However, a dynamic approach that adjusts to the post-Snowden climate should not treat the absence of reported abuse as a recipe for complacency. Instead, this is the appropriate time to put in place safeguards that will avoid abuse in the future.

External constraints should be optimal for providing flexibility while ensuring checks on potential abuse. As in other situations, a public advocate should receive notice of the NSA's use of U.S. person identifiers to query section 702 data. Once a statutory standard is in place, the advocate should be able to seek FISC review of any identifier when a reasonable possibility exists that the use of the identifier does not comply with Congress's formulation. This review would be ex post, to avoid chilling the agency's discretion in exigent situations. Ex post review would still be meaningful, given the NSA's status as a repeat player dependent on the FISC's continued good will. External constraints of this kind would assure critics that substantive standards were being followed. This external check is essential in the post-Snowden climate, in which internal "protocols" have—perhaps to a fault—become objects of corrosive cynicism.

CONCLUSION

A reform like an institutionalized public advocate's office exemplifies the fiduciary aspect of surveillance that this Article has propounded. In acting as a fiduciary, the executive must address all facets of information gathering that evolve over time: the changing threat

431. *See* United States v. Kahn, 415 U.S. 143, 157–58 (1974) (holding that the Fourth Amendment did not require the exclusion of evidence obtained by incidental collection pursuant to a warrant on an alleged bookmaker); United States v. Schwartz, 535 F.2d 160, 164 (2d Cir. 1976) (affirming the conviction of a disbarred lawyer for drug trafficking based, inter alia, on a conversation recorded pursuant to a warrant on a telephone in another person's apartment).

432. *See* PCLOB SECTION 702 REPORT, *supra* note 31, at 153–54 (separate statements of Chairman Medine and Judge Wald).

environment, technology's capacity for intrusion, technological safeguards, and perceptions of legitimacy. The frameworks enacted by Congress in section 215 and section 702 and reenacted thereafter have space for each, but changes in both provisions are necessary.

Prior to Edward Snowden's revelations, section 215's relevance standard functioned as a compromise, with restrictions on use limiting the intrusiveness of wide collection. To give the President more information about ever-changing threats, the FISC authorized broad acquisition of non-content metadata. The FISC made NSA collection conditional on the use of a narrowly tailored set of RAS-approved identifiers. Those protections leveraged technological safeguards, such as automated search protocols that courts also use in Fourth Amendment cases. The involvement of Congress and the courts addressed legitimacy concerns, although the outcry after Snowden's disclosures showed that more needed to be done. An institutionalized public advocate would be a down-payment on that debt.

The secrecy surrounding the metadata program exacerbated critics' legitimacy concerns, although here secrecy functioned in the way that the Framers had favored: secrecy enhanced strategic advantages and expanded deliberation to include approaches that disclosure would have removed from consideration. Between 2009 and June 2013, secrecy did not impede the FISC's ability to enforce the program's trade-offs between broad coverage and restricted access. It remains to be seen whether the movement toward new legislation on section 215, including the version of the USA Freedom Act passed by the House in May 2014, will strike the right balance between effectiveness and checks against abuse.

In the wake of Snowden's disclosure, even greater attention should be paid to the dual values of tailoring government access to information and ensuring the right mix of external and internal constraints. Those dual values should inform assessment of substantive changes to section 215, as well as operation of section 702. A new requirement under section 215 of a "specific selection term" related to a foreign power or agent of a foreign power may be welcome as a codification of the limited identifiers used by NSA. Defining that specific selection term, as the Leahy bill does, to include a "personal device" is appropriate, although courts must not impose an unduly narrow interpretation that limits government access to information that has previously been available by subpoena in ordinary criminal prosecutions. Under section 702, "about" collection is appropriate, given the need for government access to information on subjects involving international terrorism and other matters of foreign intelligence interest. "About" collection does not undermine the privacy rights of U.S. persons or others around the world, as long as the FISC, aided by a robust public advocate, can consider ex

post whether the selectors used are sufficiently tailored to the task. The use of U.S. person identifiers to query section 702 data raises additional issues. Here, too, a public advocate can assist the FISC. Congress should also provide greater guidance on identifiers, articulating categories such as relevance to international terrorism. These reforms will protect privacy and enhance the legitimacy of surveillance programs, without sacrificing their effectiveness.

The Leahy bill introduced in July of 2014 enhances external constraints on the NSA, but its reliance on amici curiae and certification will not be as effective as a robust public advocate. Amici curiae must be appointed by the FISC, which has signaled that it regards a voice opposing the government as disruptive and inefficient. Certification is a procedure that the Supreme Court has resisted for decades. While certification complies with Article III, it may not yield the meaningful review that the Leahy bill's drafters intended. A robust public advocate appointed by the judiciary with an ongoing role in FISC proceedings would be consistent with both Article III and the Appointments Clause, given the deference to Congress shown in *Keith* and *Morrison v. Olson*.

Snowden's revelations have reshaped national security surveillance and data collection. Those disclosures impaired the United States' ability to adjust to shifting terrorist threats. However, the debate fostered by Snowden's unauthorized actions has also provided an opportunity for deliberation about the interaction of technology, secrecy, and national security.

Tailoring and the optimal mix of external and internal constraints can build a stable framework for necessary surveillance in an uncertain world. We should not squander that opportunity.