

BYU Law Review

Volume 2016 | Issue 3


Article 4

April 2016

Quasi-Constitutional Protections and Government Surveillance

Emily Berman

Follow this and additional works at: <https://digitalcommons.law.byu.edu/lawreview>

 Part of the [Constitutional Law Commons](#), [Fourth Amendment Commons](#), and the [National Security Law Commons](#)

Recommended Citation

Emily Berman, *Quasi-Constitutional Protections and Government Surveillance*, 2016 BYU L. Rev. 771 (2016).

Available at: <https://digitalcommons.law.byu.edu/lawreview/vol2016/iss3/4>

This Article is brought to you for free and open access by the Brigham Young University Law Review at BYU Law Digital Commons. It has been accepted for inclusion in BYU Law Review by an authorized editor of BYU Law Digital Commons. For more information, please contact hunterlawlibrary@byu.edu.

Quasi-Constitutional Protections and Government Surveillance

Emily Berman^{*}

The post-Edward Snowden debate over government surveillance has been vigorous. One aspect of that debate has been widespread criticism of the Foreign Intelligence Surveillance Court (FISC), alleging that the FISC served as a rubber stamp for the government, consistently accepting implausible interpretations of existing law that served to expand government surveillance authority; engaging in tortured analyses of statutory language; and ignoring fundamental Fourth Amendment principles. This Article argues that these critiques have entirely overlooked critical aspects of the FISC's jurisprudence. A close look at that jurisprudence reveals a court that did, in fact, vigorously defend the interests customarily protected by the Fourth Amendment—individual privacy and freedom from arbitrary government intrusions into the personal sphere. Faced with government surveillance requests that posed significant privacy concerns, but for which the government was unlikely to accept “no” as an answer, the FISC resourcefully employed a familiar tool—minimization procedures (rules designed to augment privacy protections in the context of electronic surveillance)—to champion constitutional principles and preserve for itself a role in surveillance oversight while simultaneously avoiding a no-win confrontation with the executive. This creative solution took the form of a bargain: the FISC permitted the government to implement its surveillance programs, but only after embedding in those programs a set of rules protecting what I have labeled “quasi-constitutional rights.”

^{*} Assistant Professor, University of Houston Law Center. Thanks to participants in the University of Houston Law Center's Works-in-Progress Workshop, Seth Chandler, David Fagundes, Jim Hawkins, David Kwok, Peter Linzer, D. Theodore Rave, Jessica Roberts, and Joe Sanders for helpful comments, and to Barry Friedman, Aziz Huq, and Steve Vladeck for valuable conversations about the FISA Court's jurisprudence.

CONTENTS

INTRODUCTION.....	773
I. THE BULK COLLECTION CHALLENGE: THREATS TO PRIVACY IN A FOURTH AMENDMENT VOID	780
A. Bulk Telephony and Internet Metadata Collection	781
1. Internet metadata collection program: 2004-2011 .	782
2. Telephony metadata collection program: 2006- 2015	783
B. Bulk Metadata Collection and The Third-Party Doctrine	785
C. Bulk Metadata Collection and Quasi-Constitutional Rights.....	787
II. MINIMIZATION: BOLSTERING (QUASI)CONSTITUTIONAL PROTECTIONS.....	790
A. The Origins of Minimization Procedures	791
1. Criminal wiretapping minimization.....	791
2. Foreign Intelligence Surveillance Act (FISA) Minimization	794
B. Foreign Intelligence Minimization Evolves	799
1. Step one: Traditional FISA minimization	800
2. Step two: The FISA amendments act minimization	802
3. Step three: Bulk collection minimization.....	806
a. Minimization and section 702 upstream collection.....	806
b. Minimization and bulk metadata collection ...	810
(1) Bulk Internet metadata collection program minimization	811
(2) Bulk telephony metadata collection program minimization	815
III. QUASI-CONSTITUTIONAL RIGHTS: MINIMIZATION AS FOURTH AMENDMENT SUBSTITUTE	817
A. Approximating the Fourth Amendment Through Minimization.....	818
1. Prior approval	819
2. Cause	822
3. Particularity	823
B. Explaining the FISA Court's Use of Minimization in Bulk Metadata Collection Programs	825

771 *Quasi-Constitutional Protections and Government Surveillance*

1. The FISA Court’s strategic deference	825
2. The FISA Court’s quasi-constitutional rulemaking.	832
CONCLUSION	836

INTRODUCTION

The past several years have witnessed the publication (lawfully or otherwise) of an extraordinary amount of information regarding the U.S. government’s surveillance activities. Thanks to the 2013 leaks by former National Security Agency (NSA) contractor Edward Snowden, the American public is privy to an unprecedented amount of detailed information not only about the existence of surveillance programs, but also about their scope, technical details, and the formerly secret rules governing their implementation.¹ These revelations have sparked widespread public debate about the lawfulness and efficacy of the government programs, a library’s worth of commentary, a host of legal challenges in the courts, and even legislative reform.

The performance of the Foreign Intelligence Surveillance Court (FISA Court or FISC) is at the core of a significant portion of this discussion. The FISC is a federal court created by the Foreign Intelligence Surveillance Act of 1978 (FISA)² to review government applications to engage in domestic surveillance for foreign intelligence purposes.³ For the first three decades of its life, the court operated much like a magistrate judge evaluating requests for search warrants, determining (in secret and ex parte) whether government applications for surveillance authority should be approved. But today’s FISA Court does a great deal more. Since shortly after 9/11, the intelligence community’s ever-expanding surveillance powers have driven a correspondingly expanded role for the court. Rather than simply

1. The Director of National Intelligence (DNI) posts publicly available surveillance-related documents online. *IC on the Record*, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, <http://icontherecord.tumblr.com/> (last visited Oct. 21, 2016).

2. 50 U.S.C. §§ 1801–1885(c) (2012).

3. § 1803 (establishing the FISC). Originally comprised of seven judges, the court is now made up of eleven; the judges are chosen by the Chief Justice of the U.S. Supreme Court to serve seven year terms. § 1803(d). They are drawn from the existing pool of Article III judges at either the trial or appellate court level. § 1803(a). The Chief Justice also selects three judges to comprise the FISA Court of Review (FISCR), an appellate court that hears appeals from FISA Court decisions. § 1803(b). Decisions of the FISCR can be appealed to the U.S. Supreme Court. *Id.*

approving or denying applications to place individual targets under surveillance, the court has repeatedly been asked to assess the lawfulness of entire surveillance programs and secret executive branch policies.⁴

The FISC's expanded role has put the court in the position of beginning to develop what is essentially a common law of surveillance, issuing momentous opinions that evaluate questions of first impression regarding the lawfulness of the government's desired surveillance authority. Because FISA Court opinions are classified, it was only in the wake of the Snowden leaks that many of the court's previously secret decisions were exposed to the public eye. It turned out that the opinions include innovative and aggressive—some say incorrect and unconstitutional—interpretations of FISA that vastly expanded government surveillance power.

Commentators were almost universally appalled by what the FISC opinions revealed.⁵ This was particularly true of the FISC's approval

4. See *infra* Section II.B.

5. See, e.g., PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FISC (2014) [hereinafter PCLOB SECTION 215 REPORT]; REVIEW GRP. ON INTELLIGENCE AND COMM'NS TECH., LIBERTY & SECURITY IN A CHANGING WORLD (2013); ELIZABETH GOITEIN & FAIZA PATEL, BRENNAN CTR. FOR JUSTICE, WHAT WENT WRONG WITH THE FISA COURT (2014); Steven I. Vladeck, *The Case for a FISA "Special Advocate,"* 2 TEX. A&M L. REV., http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2546388; Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J. L. & PUB. POL'Y 757 (2014); Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden*, 66 HASTINGS L.J. 1, 51–57 (2014); James G. Carr, Opinion, *A Better Secret Court*, N.Y. TIMES (July 22, 2013), http://www.nytimes.com/2013/07/23/opinion/a-better-secret-court.html?_r=0; Carol Leonnig, *Secret Court Says It Is No Rubber Stamp; Work Led to Changes in U.S. Spying Requests*, WASH. POST (Oct. 15, 2013), https://www.washingtonpost.com/politics/secret-court-says-it-is-no-rubber-stamp-led-to-changes-in-us-spying-requests/2013/10/15/d52936b0-35a5-11e3-80c6-7e6dd8d22d8f_story.html; Glenn Greenwald, *FISA Court Oversight: A Look Inside a Secret and Empty Process*, THE GUARDIAN (June 18, 2013), <https://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy>; Andrew Weissman, *The Foreign Intelligence Surveillance Court: Is Reform Needed?*, JUSTSECURITY.ORG (June 12, 2014), <https://www.justsecurity.org/11540/guest-post-foreign-intelligence-surveillance-court-reform-needed/>; Orin Kerr, *My (Mostly Critical) Thoughts on the August 2013 FISC Opinion on Section 215*, VOLOKH CONSPIRACY (Sept. 17, 2013, 7:39 PM), <http://volokh.com/2013/09/17/thoughts-august-2013-fisc-opinion-section-215/>. The court did have its defenders, but they were a decided minority. See e.g., PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., WORKSHOP REGARDING SURVEILLANCE PROGRAMS OPERATED PURSUANT TO SECTION 215 OF THE USA PATRIOT ACT & SECTION 702 OF THE FISC (2013) (statements

of two so-called “bulk metadata” programs, which collected and stored vast amounts of information about Americans’ domestic emails and phone calls.⁶ The gist of the criticism was that the court had been no more than a rubber stamp for the government, consistently accepting executive-branch interpretations of FISA, no matter how implausible, that expanded government surveillance authority; engaging in tortured analyses of statutory language; failing to impose sufficient sanctions on the government when it broke the rules; and ignoring fundamental Fourth Amendment principles.⁷

This Article argues that these critiques have entirely overlooked critical aspects of the FISA Court’s jurisprudence. A close look at that jurisprudence reveals a court that did, in fact, vigorously defend the interests customarily protected by the Fourth Amendment—individual privacy and freedom from arbitrary government intrusions into the personal sphere—albeit through unorthodox means. In fact, faced with surveillance requests that posed significant privacy concerns, but for which the executive was unlikely to accept no as an answer, the court was able to craft a creative means of championing constitutional principles while simultaneously avoiding a confrontation with the executive that it could not win. This solution took the form of a bargain: the FISC permitted the government to implement its surveillance programs, but only after embedding in

of Raj De, NSA General Counsel, Robert Litt, ODNI General Counsel); PCLOB REPORT SECTION 215, *supra* (minority views).

6. *See infra* Section I.A. “Metadata is . . . data about data or information about information.” NATIONAL INFORMATION STANDARDS ORGANIZATION, UNDERSTANDING METADATA 1 (2004), <http://www.niso.org/publications/press/UnderstandingMetadata.pdf>. Communication metadata is information about a communication itself, including session identifying information (for example, originating and terminating telephone number or email address and communications device identifiers like IP addresses), routing information, and time and duration of calls. *See infra* Section I.A. “Bulk” collection—in contrast to “targeted” collection—is collection where a significant portion of the collected data is *not* associated with specific targets relevant to a particular investigation. *See infra* Section I.A. Unlike targeted surveillance, approval of bulk surveillance does not involve case-by-case judicial assessments of the validity of each proposed target. *See infra* Section II.B.

7. The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,” and provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. CONST. amend. IV.

those programs a set of rules protecting what I have labeled “quasi-constitutional rights.”⁸

By quasi-constitutional rights, I mean an individual’s interest in preserving principles ordinarily protected by the Constitution—privacy, for example—regardless of whether the Constitution *itself* protects those interests. In other words, they are interests that may not be protected by a strict application of existing constitutional *doctrine*, but that are nevertheless inherent in fundamental constitutional *values*.

The government’s bulk metadata collection programs provide an example.⁹ These programs did not collect the *content* of communications, which unquestionably enjoys Fourth Amendment protections. Instead, at issue was non-content information—metadata—about phone calls and email, including which email addresses or phone numbers communicated with one another, when those conversations took place, how long they lasted, and the like. Due to a controversial doctrine—the third party doctrine—the Fourth Amendment does not apply to communications metadata because “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties”—here, the phone company.¹⁰ So the usual privacy safeguards compelled by the Constitution do not apply. Under the best of circumstances, the third party doctrine raises significant privacy concerns. After all, an individual’s desire to shield from government scrutiny the list of people with whom she exchanges phone calls or emails does not seem unreasonable. The bulk collection programs multiply these privacy concerns exponentially. Rather than collecting the metadata of one individual who is relevant to an investigation, the federal government collected *everyone’s* metadata—all records regarding phone calls or emails where at least one end of the communication was in the United States.¹¹ Collecting and

8. The term is borrowed from William N. Eskridge, Jr. & Philip P. Frickey, *Quasi-Constitutional Law: Clear Statement Rules as Constitutional Lawmaking*, 45 VAND. L. REV. 593 (1992).

9. See *infra* Section I.A.

10. *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979); see also *infra* Section I.B (discussing the third party doctrine in more detail).

11. An order compelling one company to provide its telephony metadata to the government requires the phone company to provide, “on an ongoing daily basis,” all international *and* domestic call detail records. *In re* Application of the FBI for an Order Requiring the Production of Tangible Things From Verizon Bus. Network Servs., Inc. on Behalf

analyzing data in bulk allows the government to glean much more information about our lives than isolated bits of information would permit. The privacy implications of bulk metadata collection are therefore profound. Nevertheless, the FISA Court accepted the government's argument that metadata remains outside the Constitution's protection, regardless of the volume in which it is collected.¹²

In evaluating the government's applications to implement these programs, the FISA Court found itself faced with two unappealing options. One was to reject the government's argument that the third party doctrine controlled, insist that the usual Fourth Amendment rules applied,¹³ and thereby provoke a constitutional confrontation with the executive. The other was simply to approve the bulk collection programs without constraints despite their privacy implications. Refusing to limit itself to these undesirable options, the FISA Court was able to chart a third course: It vindicated individual privacy interests *without* challenging the government's interpretation of the Constitution by treating those interests as *quasi*-constitutional rights, protecting them with measures that furthered the constitutional value of privacy, while at the same time declaring the Constitution itself inapplicable.

The mechanism through which the FISA Court accomplished this feat is a decades-old privacy-protection tool known as minimization.¹⁴ The idea behind minimization is a simple one: Some means of government investigation pose such serious threats to Americans' privacy and such heightened potential for government abuse that their implementation must include procedures to guard against overbroad collection, as well as improper use of information once it is in the

of MCI Commc'n Servs., Inc., No. BR 13-80, Secondary Order, at 1-2 (FISA Ct. Apr. 25, 2013).

12. See *infra* note 63 and accompanying text.

13. One district court judge did exactly that. *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013).

14. There are statutory provisions defining minimization procedures in a variety of contexts. 50 U.S.C. § 1801(h) (2012) (electronic communications); *id.* § 1861(g) (the collection of tangible things); *id.* § 1821 (for physical searches). As of June 2015, collection using a pen register or trap-and-trace device (a device that provides information about incoming or outgoing communications, respectively) must be employed with "[p]rivacy procedures." *Id.* § 1842(h).

government's possession.¹⁵ In other words, the procedures are a way to impose a "set of controls on data to balance privacy and national security interests."¹⁶ In their traditional form, minimization procedures are included in the electronic surveillance privacy protections demanded by the Fourth Amendment. For most searches or seizures, the Supreme Court has held that a warrant is valid if it is issued by a neutral magistrate on a showing of probable cause, describing the things to be seized and the places to be searched with particularity.¹⁷ Searches and seizures carried out pursuant to warrants that comply with these requirements are presumptively considered consistent with the Fourth Amendment. The same requirements are *necessary* but not *sufficient*—as a constitutional matter—for searches or seizures that employ electronic surveillance. So when Congress statutorily approved electronic surveillance as an investigative tool—first for criminal investigations and then for foreign intelligence collection—it augmented those traditional warrant requirements with additional safeguards, the most important of which is minimization.¹⁸

The years since FISA authorized electronic surveillance for foreign intelligence purposes have seen an evolution both in surveillance law itself and in the role of minimization.¹⁹ Post-9/11 counterterrorism concerns and transformational technological advancements in collection and analysis capability have driven a significant expansion of surveillance powers in the last decade. Along with this expansion has come a diminution of the rigorousness with which the usual warrant prerequisites constrain surveillance activities.²⁰ As these more traditional limits have fallen away, courts have filled the resulting gaps

15. For example, when using a wiretap to collect communications in a criminal investigation, minimization procedures might require the government to limit recording to those conversations in which the target of surveillance is a participant. If the target's fourteen-year-old daughter calls a friend, by contrast, the government must not record (or must destroy the recording of) that conversation.

16. PRIVACY & AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FISA 50 (2014) [hereinafter PCLOB SECTION 702 REPORT].

17. *Dalia v. United States*, 441 U.S. 238, 255 (1979) (citations omitted).

18. See *infra* Section II.A.

19. See Emily Berman, *The Two Faces of the Foreign Intelligence Surveillance Court*, 91 IND. L.J. 1191, 1196–1202 (2016).

20. *Id.*

with minimization rules.²¹ The result is that minimization has become more and more central to the protection of constitutional values over time.²² This evolution culminated in the use of minimization in the bulk metadata collection programs, where the FISA Court determined that *no* traditional safeguards applied.²³ To fill this void, the court used minimization to *approximate* customary Fourth Amendment limits as a means of protecting quasi-constitutional privacy rights.

Seen in this light, the FISA Court's use of minimization procedures to protect quasi-constitutional privacy rights is simply a creative adaptation of a 20th century judicial tool to address a 21st century surveillance challenge. Indeed, this adaptation raises the question whether the FISC's use of minimization might provide insight into how to meet some of the other daunting challenges presented by trying to adapt Fourth Amendment doctrine to the digital age.²⁴ Minimization's *raison d'être* has always been to bolster traditional safeguards against unreasonable government intrusions on individual privacy. There is no reason its benefits should be limited to the electronic surveillance context. Whatever its utility elsewhere, however, the value of minimization here is not speculative. By casting minimization in its familiar role as a shield for individual privacy in the context of bulk collection, the FISC was able to succeed in both furthering individual privacy interests and preserving for itself an oversight role in circumstances where the Constitution guaranteed neither.

This Article proceeds in three parts. Part I sets out one of the fundamental challenges posed by the government's bulk metadata collection programs: They represent significant threats to individual privacy, as illustrated in Section A, yet, as Section B explains, are not constrained by the traditional constitutional protections designed to

21. Minimization has always been the courts' domain. Surveillance laws have consistently tasked courts with ensuring that minimization procedures are appropriate. 50 U.S.C. § 1881a(i) (2012). Moreover, judges have been integral in monitoring the government's compliance with those procedures. *Id.* The judiciary is therefore well versed in tailoring minimization procedures to the needs of specific instances of surveillance.

22. *See infra* Section II.B.

23. *See infra* Section I.B (discussing third party doctrine and its relevance to bulk metadata collection).

24. Whether the FISA Court's use of minimization can truly suggest ways to address other Fourth Amendment challenges requires further study, in which I hope to engage in future work. *See infra* note 85 (noting that other scholars have suggested use of minimization-like procedures to increase privacy protections for digital information).

safeguard privacy interests. Section C shows that this seeming contradiction is not lost on the FISA Court. Part II then introduces the tool designed to mitigate the threats to privacy inherent in electronic surveillance programs: minimization. Section A examines the constitutional roots of minimization procedures, demonstrating that from their genesis they were meant to ensure that electronic surveillance programs would respect constitutional boundaries. Section B then shows that as the nature of surveillance—and the role of the FISC itself—has changed over time, robust minimization rules have become more and more central to the court’s efforts to protect individual rights. This evolution culminated with the FISA Court’s application of the decades-old privacy-protection tool of minimization to the decidedly new context of bulk metadata collection in order to protect quasi-constitutional privacy rights. Finally, Part III argues that the FISC’s use of minimization represents a carefully calibrated compromise. The FISA Court acceded to the government’s argument that the Constitution itself was inapplicable, while at the same time imposing minimization procedures that approximated traditional Fourth Amendment protections. In other words, the FISC used minimization to create a delicate balance that avoided a clash with the executive branch, yet succeeded both in subjecting bulk metadata collection to meaningful limits and in retaining a role for itself in surveillance oversight.

I. THE BULK COLLECTION CHALLENGE: THREATS TO PRIVACY IN A FOURTH AMENDMENT VOID

This Part examines how bulk collection programs simultaneously pose threats to individual privacy interests—interests that I refer to as quasi-constitutional rights—yet evade constitutional scrutiny. Section A reveals the significance of the privacy threat that these programs represent by detailing the unprecedented scope of surveillance that they allow. Section B then explains how the third party doctrine arguably renders traditional constitutional protections inapplicable in this context. Finally, Section C shows that the FISA Court was fully aware of the dilemma these two realities created. Otherwise-inexplicable portions of the court’s opinions authorizing bulk collection make perfect sense if they are seen as implicit recognition of the need to protect quasi-constitutional privacy rights.

A. Bulk Telephony and Internet Metadata Collection

The bulk collection of information is the antithesis of the type of targeted collection normally required by the Fourth Amendment. In fact, the very point of a bulk collection program is to identify as-yet unknown terrorism suspects, who can then be subjected to more particularized targeting. It is the analysis of information gathered in bulk that allows the government to identify individuals, phone numbers, or email addresses that are associated with international terrorist organizations. If the government could already identify such targets with particularity, it would not need to populate and analyze the bulk databases.

Because they are designed for broad, rather than targeted and particularized surveillance, bulk collection programs will lack the procedural protections provided by traditional warrant requirements. There is no criterion for which the government must demonstrate probable cause nor can the evidence to be seized be identified with any particularity. Collection might be confined to a particular *category* of information—e.g., telephony or Internet metadata—but the particularity will be no more granular than that.²⁵ And since the government need not demonstrate probable cause or particularity, there is no role for a neutral magistrate to consider whether those requirements are met. As a result, the usual restraints that prevent the government from seeking or using irrelevant information about innocent individuals are absent. The government may collect and analyze unprecedented amounts of information about U.S. persons' communications, but without concomitant safeguards against infringing on individual privacy.

The government has engaged in (at least) two bulk metadata collection programs—the bulk collection of Internet and telephony metadata, respectively. These programs represented novel, aggressive—many would say erroneous—interpretations of the relevant statutory provisions and vastly expanded the scope of

25. The bulk Internet collection program was tailored (in some way that is redacted) “in order to build a meta data archive that will be, in relative terms, richly populated with [redacted] related communications.” *In re* [REDACTED], No. PR/TT [REDACTED], Opinion and Order, at 47 (FISA Ct. July 14, 2004) [hereinafter FISC’s Pen/Trap Opinion]. Nevertheless, the FISC recognizes that the communications of non-terrorists will be also collected in order to obtain the critical foreign intelligence information that the government seeks. *Id.* at 49 n.34.

permissible government surveillance. The intention of the programs was to allow the government to “identify communications among known and unknown terrorism suspects,” with a particular focus on locating any such suspects inside the United States.²⁶

1. Internet metadata collection program: 2004-2011

In the first program, the federal government sought authorization from the FISA Court to engage in bulk collection of Internet metadata—including metadata about Americans’ domestic emails—using the FISA pen register and trap-and-trace (“pen/trap”) provision.²⁷ This provision is ordinarily used to collect communications metadata—dialing, routing, addressing, or signaling information—to or from a particular individual or communication device. To get FISA Court approval for a pen/trap order seeking metadata from an identified individual, the government must certify “that the information likely to be obtained is foreign intelligence information . . . or is relevant to an ongoing investigation.”²⁸

When it came to the bulk collection program, however, the government proposed (and the FISC allowed) using the pen/trap provision as authority to collect communications metadata not simply to or from one person or communications device. Instead, it asked the FISA Court to adopt an aggressive interpretation of the pen/trap provision that would allow the collection of such metadata in bulk—including (at least) email routing and addressing information—as it transited the Internet.²⁹

The FISA Court recognized that the government was requesting an “exceptionally broad form of collection” in which “only a very

26. PCLOB SECTION 215 REPORT, *supra* note 5, at 8.

27. Pen registers record information about outgoing phone calls; trap-and-trace devices record information about incoming calls. *See* 50 U.S.C. § 1841(2) (2012) (referring to 18 U.S.C. § 3127 for the definitions of “pen register” and “trap and trace device”). The government shut this program down in “2011 for ‘operational and resource reasons.’” Charlie Savage, *File Says N.S.A. Found Way to Replace Email Program*, N.Y. TIMES (Nov. 19, 2015), http://www.nytimes.com/2015/11/20/us/politics/records-show-email-analysis-continued-after-nsa-program-ended.html?_r=0. *But see id.* (reporting that the NSA found a “functional equivalent” for the program overseas, where the NSA is subject to fewer oversight restrictions).

28. 50 U.S.C. § 1842(c)(2).

29. *See* PCLOB SECTION 215 REPORT, *supra* note 5, at 38; FISC’s Pen/Trap Opinion, *supra* note 25.

small percentage” of the Internet metadata collected would be “directly relevant” to an investigation.³⁰ Nevertheless, the court accepted the government’s argument that such collection satisfied the statutory requirement that the information be “relevant to an ongoing investigation” by adopting a remarkably expansive definition of “relevant.”³¹ According to the FISC opinion, because large-scale collection of metadata was “necessary to identify the much smaller number” of communications related to terrorism, all of that metadata was “relevant” to a counterterrorism investigation.³² With relevance so defined, the program permitted the acquisition of vast amounts of (untargeted) metadata about Internet communications, such as email, even if those communications were purely domestic, i.e., from one American to another.

Once the NSA captured the communications metadata, it was stored in a government database.³³ Analysts could then “query,” or search, the database using terms, known as “seed identifier[s]” (usually email addresses), in an effort to identify as-yet-unknown terrorist suspects through “contact chaining”—the process of analyzing communications patterns of targets and their associates to locate individuals who might be in contact with known terrorists.³⁴ So the NSA collected and retained a giant haystack of information about domestic email traffic in the hope that it would lead them to a needle—a terrorist operating inside the U.S.

2. *Telephony metadata collection program: 2006-2015*

The second program, which collected in bulk domestic telephony metadata, had similar goals, but was more controversial than the pen/trap program. The telephony metadata program operated pursuant to a FISA Court order under section 215 of the USA

30. FISC’s Pen/Trap Opinion, *supra* note 25, at 23, 48.

31. *Id.* at 48–50 (quoting 50 U.S.C. § 1842(c)(2)).

32. *Id.* at 23, 48. This definition of “relevant” proved particularly controversial. *See, e.g.*, PCLOB SECTION 215 REPORT, *supra* note 5, at 38.

33. *See* Exhibit A: Declaration of General Keith B. Alexander, United State Army, Director of the National Security Agency at 14–15, 24, [REDACTED] (FISA Ct. [REDACTED]) (No. PR/TT).

34. *Id.* at 3–4, 17–20; *see also* PCLOB SECTION 215 REPORT, *supra* note 5, at 146 (describing the limited utility of this tool).

PATRIOT Act, also known as the FISA “business records provision.”³⁵ Like the pen/trap provision, section 215 was not drafted to authorize the collection of vast databases of metadata; it contemplated more individualized targeting.³⁶ To secure an order under section 215’s authorization for the collection of “any tangible things,” the government must demonstrate to a FISA judge—by a statement of specific, articulable facts—that there are “reasonable grounds to believe that the tangible things sought are relevant” to an ongoing terrorism or espionage investigation.³⁷ Section 215 could be used to seize, for example, an individual’s banking records or his home computer.

Under section 215’s bulk collection program (also referred to as the telephone metadata program or the telephone bulk collection program), however, the NSA did not seek out tangible things related to a specific target. Instead, it relied upon the Internet metadata opinion’s expansive definition of relevance to again acquire massive amounts of information about Americans’ communications.³⁸ The information collected—nearly all call detail records generated by certain telephone companies in the United States—included much of the information that typically appears on a customer’s telephone bill: the date, time, and duration of a call as well as the participating telephone numbers.³⁹ The FISA Court’s orders required communications providers to supply virtually all of their calling records to the NSA, the vast majority of which relate to purely

35. PCLOB SECTION 215 REPORT, *supra* note 5, at 21–22; *see also* 50 U.S.C. § 1861(a)(1) (2012) (stating that the FBI “may make an application for an order requiring the production of any tangible things . . . for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities”). The government continued this program until Congress legislatively barred bulk collection in the USA Freedom Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015).

36. PCLOB SECTION 215 REPORT, *supra* note 5, at 57–102 (explaining why FISC’s interpretation of the statutory text of section 215 is overbroad).

37. 50 U.S.C. § 1861(b)(2)(A).

38. ADMIN. WHITE PAPER, BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 8–9 (2013) (“Specifically, in the circumstance where the Government has reason to believe that conducting a search of a broad collection of telephony metadata records will produce counterterrorism information—and that it is necessary to collect a large volume of data in order to employ the analytic tools needed to identify that information—the standard of relevance under Section 215 is satisfied.”).

39. *Id.* at 3.

domestic calls—calls in which both participants are located within the United States.⁴⁰ As a result, the program yields metadata for an enormous volume of telephone communications. The NSA, in fact, has said that the bulk collection program allowed “‘comprehensive’ analysis of telephone communications ‘that cross different providers and telecommunications networks.’”⁴¹ Then, as with the Internet metadata program, the NSA stored the call detail records in a centralized database, which analysts could query using seed identifiers (here, usually phone numbers) and apply contact chaining to seek out individuals with terrorist connections.⁴²

These bulk metadata collection programs authorized the acquisition of domestic communications metadata on an unprecedented scale.⁴³ Ordinarily, such intrusive surveillance would be constrained by limits imposed by the Fourth Amendment. But as the next Section explains, despite the breadth of the collection—and the threats to privacy that such untargeted surveillance represents—Fourth Amendment rules were determined to be inapplicable.

B. Bulk Metadata Collection and the Third-Party Doctrine

When it comes to electronic communications metadata, the government maintains—and the FISC has agreed—that constitutional protections simply do not apply.⁴⁴ Instead, the information qualifies as third party records in which, according to the third party doctrine, Americans have no reasonable expectation of privacy.⁴⁵ The third party

40. PCLOB SECTION 215 REPORT, *supra* note 5, at 22.

41. *Id.*

42. *Id.* at 26–31. After the section 215 program became public in 2013, President Obama slightly curtailed its scope; the USA Freedom Act of 2015 then enacted several modifications to section 215 itself, including a bar on bulk collection. See Jennifer Steinhauer & Jonathan Weisman, *Key Parts of Patriot Act Expire Temporarily as Senate Moves Toward Limits on Spying*, N.Y. TIMES (May 31, 2015), <http://www.nytimes.com/2015/06/01/us/politics/senate-nsa-surveillance-usa-freedom-act.html>; Jennifer Steinhauer & Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 Is Sharply Limited*, N.Y. TIMES (June 2, 2015), <http://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html>.

43. See, e.g., *ACLU v. Clapper*, 785 F.3d 787, 821 (2d Cir. 2015).

44. FISC’s Pen/Trap Opinion, *supra* note 25, at 58–66; *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted]*, No. BR 13-109, Amended Memorandum Opinion, at 5–9 (FISA Ct. Aug. 29, 2013).

45. FISC’s Pen/Trap Opinion, *supra* note 25, at 58–66; *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted]*, No. BR 13-109, at 5–9.

doctrine, which the Supreme Court created in a series of opinions in the 1970s,⁴⁶ provides that information voluntarily revealed to a “third part[y],” a term encompassing any individual or non-government institution, enjoys no Fourth Amendment protection.⁴⁷ Having relinquished this information to another, the doctrine reasons, you have no reasonable expectation that it will remain private.⁴⁸ The Constitution simply does not regulate the government’s collection or use of that information.⁴⁹ No warrant is required to seize it, and government officials engage in no constitutional infraction by collecting and examining it.⁵⁰

To be sure, the third party doctrine has received a lot of (well-deserved) criticism over the years.⁵¹ Some have decried the doctrine since its inception.⁵² But recently, these complaints have become a chorus. The more we live our lives online, the argument goes, the more information we entrust to third parties. This argument has two implications. First, more and more of what used to be considered private papers are now considered third party records.⁵³ Do we really have no expectation of privacy in the files in our Dropbox accounts? Or in our shopping history with Amazon? Second, the government’s technological capacity to aggregate and mine a large volume of data means that metadata often will be at least as revealing as communications content.⁵⁴

In a recent concurrence, Justice Sonya Sotomayor argued that “it may be necessary to reconsider” the third party doctrine because it is “ill-suited to the digital age, in which people reveal a great deal of

46. *E.g.*, *United States v. Miller*, 425 U.S. 435, 443–45 (1976).

47. *Smith v. Maryland*, 442 U.S. 735, 743–45 (1979).

48. *Id.*

49. *See id.* at 744–46.

50. *See id.*

51. As Professor Orin Kerr explained, “A list of every article or book that has criticized the doctrine would make this the world’s longest law review footnote” (and that’s saying something!). Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 n.5 (2009) (listing some critiques of the third party doctrine).

52. *E.g.*, *Smith*, 442 U.S. at 746–48 (Stewart, J., dissenting).

53. *See* Michael W. Price, *Rethinking Privacy: Fourth Amendment “Papers” and the Third-Party Doctrine*, 8 J. NAT’L SEC. L. & POL’Y 247, 265–66, 268–76 (2016).

54. *E.g.*, *United States v. Jones*, 132 S. Ct. 945, 956–57 (2012) (Sotomayor, J., concurring); *see also* Donohue, *supra* note 5, at 873 (recognizing that “[s]ophisticated data-mining and link-analysis programs can . . . analyze . . . information . . . more quickly, deeply, and cheaply than” ever before).

information about themselves to third parties in the course of carrying out mundane tasks.”⁵⁵ As the justice points out, sometimes a person’s digital trail can generate “a wealth of detail about her familial, political, professional, religious, and sexual associations.”⁵⁶ This is true even of communications metadata. What is more intrusive, listening to one private phone conversation or amassing a list of emails or phone calls to a psychiatrist; an abortion clinic; a defense attorney; or a mosque, synagogue, or church? The government need not access the contents of any of those communications to glean information that an individual might wish to keep confidential.

The government has always maintained that the third party doctrine applies with full force to any form of communications metadata, even when collected in bulk. Because both the Internet and telephony bulk collection programs collected only metadata, the government and the FISC considered the Fourth Amendment inapplicable to the information in the resulting databases.⁵⁷

C. Bulk Metadata Collection and Quasi-Constitutional Rights

Despite the purported inapplicability of the Constitution to the information acquired through the bulk collection programs,⁵⁸ the FISC’s bulk collection orders exhibit a decided solicitude for the very same interests with which the Fourth Amendment is concerned—individual privacy and freedom from arbitrary government intrusions. The FISC clearly recognized that bulk collection of metadata implicates many of the same concerns as those raised by the collection of content. At several points in the FISC’s opinion approving bulk Internet collection, in particular, the court’s reluctance to eschew subjecting the program to constitutional scrutiny is evident.

First, the court repeatedly articulated serious concerns about the unprecedented scope of the “exceptionally broad form of collection” that the government requested.⁵⁹ The exact parameters of the program

55. *Jones*, 132 S. Ct. at 957.

56. *Id.*

57. I agree that metadata collected in bulk should enjoy the same Fourth Amendment protection as communications content. This Article, however, aims to analyze the FISA Court’s bulk metadata jurisprudence as it *is*, not as it *should* be.

58. *See supra* Section I.B.

59. FISC’s Pen/Trap Opinion, *supra* note 25, at 23.

remain classified, but the FISC noted both the size of the program and its breadth, pointing out that the “raw volume of the proposed collection is enormous,”⁶⁰ and that it permits the government to acquire “meta data pertaining to . . . communications of United States persons located within the United States who are not the subject of any FBI investigation.”⁶¹ As a result, the court concluded, the program “carries with it a heightened risk that collected information could be subject to various forms of misuse.”⁶² In other words, metadata collected in bulk implicates the same constitutionally-inspired concerns about privacy and constraint of government action that animate the Fourth Amendment’s warrant requirement.

Having identified concerns similar to those behind Fourth Amendment protections—quasi-constitutional concerns—the FISA Court goes on to say that despite the fact that “this application involves unusually broad collection and distinctive modes of analyzing information, . . . no Fourth Amendment search or seizure is involved.”⁶³ Collecting information in which no individual has a reasonable expectation of privacy—like metadata—from a large number of people, it opines, does not change the fact that the Constitution does not protect that information.⁶⁴ In other words, unprotected information collected from a vast number of individuals is still unprotected information.

Yet, the next page of the opinion rejects the very same idea through an analogy to courts’ evaluation of privacy concerns in the Freedom of Information Act (FOIA)⁶⁵ context. The court points out that under FOIA, “[t]he public disclosure of aggregated and compiled data has been found to impinge on privacy interests . . . even if the information was previously available to the public in a scattered, less accessible form.”⁶⁶ So the court is not blind to the fact that collecting

60. *Id.* at 39.

61. *Id.* (quoting government application).

62. *Id.* at 68.

63. *Id.* at 62.

64. *Id.* at 63 (“So long as no individual has a reasonable expectation of privacy in meta data, the large number of persons whose communications will be subjected to the proposed pen register/trap and trace surveillances is irrelevant to the issue of whether a Fourth Amendment search or seizure will occur.”).

65. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974).

66. FISC’s Pen/Trap Opinion, *supra* note 25, at 64 n.47.

many pieces of data from disparate sources and aggregating them for analysis may raise concerns not implicated by any isolated piece of information.

Another spot where quasi-constitutional reasoning seeps into the court's reasoning is in its statutory analysis. The primary statutory question is whether Internet information collected in bulk qualifies as "relevant" to an ongoing terrorism investigation.⁶⁷ In determining that the "relevance standard does not require a statistical 'tight fit' between the volume of proposed collection and the much smaller proportion of information that will be directly relevant" to investigations,⁶⁸ the FISC engages in what can only be described as a Fourth Amendment analysis of the program. The court explains this analysis by stating that it "finds instructive Supreme Court precedents on when a search that is not predicated on individualized suspicion may nonetheless be reasonable under the Fourth Amendment."⁶⁹ It is difficult to determine why the statutory question whether the metadata is relevant to an ongoing terrorism investigation leads the court to ask whether the government program passes a Fourth Amendment reasonableness analysis. Yet the court goes on to consider that very question.⁷⁰

The opinion's ambivalence toward the relevance of Fourth Amendment doctrine is again on display in the court's application of a Fourth Amendment balancing test to the program. Determining the Fourth Amendment reasonableness of a search or seizure requires courts to weigh, under the totality of the circumstances, the government's interest in the search or seizure against the individual's interest in privacy.⁷¹ Here, the court recognized the government's interest as the need to identify and track terrorist suspects so as to thwart terrorist attacks, an interest that "clearly involves national security interests . . . and is at least as compelling as other governmental interests that have been held to justify searches in the

67. *Id.* at 48.

68. *Id.* at 49–50.

69. *Id.* at 50; *see also id.* at 50 n.35 ("[T]he Court agrees with the Government's suggestion that the balancing methodology used to assess the reasonableness of a Fourth Amendment search or seizure is helpful in applying the relevance standard to this case.").

70. *Id.* at 50–51.

71. *See, e.g.,* *Camara v. Mun. Court*, 387 U.S. 523, 534–39 (1967).

absence of individualized suspicion.”⁷² But on the other side of the balance—the individual’s interest in privacy—the court asserts that “meta data is not of a stature protected by the Fourth Amendment,” so the individual interest is minimal.⁷³ This weighs the government’s interest in national security against a non-existent interest in the privacy of metadata. If the interest on the individual’s side of the scale is truly weightless, why engage in balancing at all?

The logical explanation for all of these elements of the FISC’s opinion is that despite the allegedly unprotected nature of metadata, the FISC realized that permitting the government to aggregate and data mine communications metadata collected in bulk without constraints designed to protect privacy interests was untenable. Having recognized that the collection both raises (quasi) constitutional concerns and escapes traditional constitutional scrutiny, the court turned to a time-tested means of safeguarding privacy interests in the electronic surveillance context: minimization.

II. MINIMIZATION: BOLSTERING (QUASI-)CONSTITUTIONAL PROTECTIONS

This Part tracks the evolution of minimization requirements from their origins in constitutional doctrine to their contemporary use. It will demonstrate in Section A that the very concept of minimization was to create a tool that would supplement traditional Fourth Amendment procedures because those procedures alone failed to alleviate the privacy threat posed by electronic surveillance. Minimization procedures therefore became obligatory in that context, with the courts assigned the case-by-case role of determining how much minimization (and in what form) each individual circumstance required. Section B shows that over time minimization procedures became more and more integral to the FISA Court’s efforts to plug the privacy gaps that emerged as a result of expanded government surveillance authority. The FISA Court’s invocation of minimization procedures to protect quasi-constitutional rights in the bulk metadata context was merely the latest in a series of resourceful adaptations of a familiar tool to circumstances that minimization’s architects never could have anticipated.

72. FISC’s Pen/Trap Opinion, *supra* note 25, at 51–52.

73. *Id.* at 51.

A. The Origins of Minimization Procedures

This Section tells the story of how minimization procedures were devised as a tool for constitutional protection in the context of criminal wiretapping and were then imported—in amplified form—into the foreign intelligence context.

1. Criminal wiretapping minimization

By the mid-1960s, technological advances and increased efforts to fight crime—and in particular organized crime—had prompted law enforcement to employ new methods of investigation. Given the difficulty of finding witnesses willing to testify on the government’s behalf against mafia-connected defendants, wiretaps had become “an indispensable aid to law enforcement.”⁷⁴ The rules governing use of these tactics were, however, unclear. The President’s Commission on Law Enforcement and Administration of Justice, a panel appointed by President Johnson in 1965 to “examine every facet of crime and law enforcement in America,”⁷⁵ noted that “[t]he state of the law in this field is so thoroughly confused that no policeman, except in States that forbid both [wiretapping and eavesdropping] totally, can be sure about what he is allowed to do.”⁷⁶ One of the Commission’s many recommendations was that “Congress should enact legislation dealing specifically with wiretapping.”⁷⁷

Congress took up the challenge issued by the President’s Commission, but not before the Supreme Court had weighed in. *Berger v. New York* struck down New York State’s wiretapping law, holding that it was insufficiently protective of the Fourth Amendment.⁷⁸ In that opinion, the Supreme Court “laid out guidelines for the Congress and State legislatures to follow in enacting

74. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 801(c), 82 Stat. 211 (1968); *see also* PRESIDENT’S COMM’N ON LAW ENF’T & THE ADMIN. OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 201 (1967) [hereinafter THE CHALLENGE OF CRIME IN A FREE SOCIETY] (noting that New York County’s District Attorney “testified that electronic surveillance is: ‘the single most valuable weapon in law enforcement’s fight against organized crime’”).

75. Nicholas deB. Katzenbach, *Foreword* to THE CHALLENGE OF CRIME IN A FREE SOCIETY, *supra* note 74.

76. THE CHALLENGE OF CRIME IN A FREE SOCIETY, *supra* note 74, at 94.

77. *Id.* at 203.

78. *Berger v. New York*, 388 U.S. 41, 44 (1967).

wiretapping and electronic eavesdropping statutes which would meet constitutional requirements.”⁷⁹ In drafting what would ultimately become Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III),⁸⁰ Congress recognized that any federal wiretapping legislation would have to conform to the constitutional limits articulated in *Berger*.⁸¹ As a result, drafts of the bill were “tailored to meet the constitutional requirements imposed by” the Supreme Court.⁸² Thus, Congress viewed the procedural safeguards ultimately included in Title III’s wiretapping rules as constitutionally required.⁸³

The law included the obligations usually present in the Fourth Amendment warrant context (probable cause, particularity, and review by a neutral magistrate⁸⁴), but Congress also inferred an obligatory additional procedural protection from the Supreme Court’s jurisprudence: minimization. Title III was the first use of what are now known as minimization procedures.⁸⁵ Specifically, Title III requires

79. S. REP. NO. 90-1097, at 68 (1968).

80. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 211–25 (1968) (codified at 18 U.S.C. §§ 2510–2520 (2012)).

81. *See, e.g.*, S. REP. NO. 90-1097, at 224 (views of Senators Dirksen, Hruska, Scott, and Thurmond).

82. *Id.* The proposed legislation was also modified to comply with *Katz v. United States*, 389 U.S. 347, 352–53 (1967) (finding that conversations in phone booths are entitled to Fourth Amendment protection).

83. *E.g., id.* at 75 (“[T]he subcommittee has used the *Berger* and *Katz* decisions as a guide in drafting [T]itle III.”); *see also id.* at 28 (“This proposed legislation conforms to the constitutional standards set out in *Berger v. New York*, and *Katz v. United States*.” (citations omitted)); *id.* at 238 (individual views of Senators Dirksen, Hruska, Scott, and Thurmond) (pointing out that “[n]othing the Supreme Court said in either *Berger* or *Katz* indicates that” the use of wiretapping must be limited to the investigation of a limited number of enumerated offenses, thereby recognizing that *Berger* and *Katz* do indicate that the other procedural limits contained in the bill *are* necessary).

84. *See supra* note 17 and accompanying text.

85. It is interesting to note that some commentators have turned to mechanisms that could reasonably be called minimization procedures in the search for limiting principles on the government’s collection and use of electronic data that enjoys full Fourth Amendment protection. These arguments take as a given that, whether it is a good thing or not, “the ship has already sailed with regard to the *collection* of Big Data.” Stephen I. Vladeck, *Big Data Before and After Snowden*, 7 J. NAT’L SEC. L & POL’Y 333, 335 (2014). The true debate in the digital age has become how to restrict the ways that data may be used. *Id.*; Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 388 (2015) (noting that acquisition and use restrictions “must go hand-in-hand”); Deven R. Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 NOTRE DAME L. REV. 579, 625 (2014) (arguing for time limits on the use of data); Stephen E. Henderson, *Our Records Panopticon and*

that every wiretap order “shall contain a provision that the authorization to intercept shall be . . . conducted in such a way as to minimize the interception of communications not otherwise subject to interception.”⁸⁶ As several Supreme Court justices pointed out on more than one occasion,

[the] “minimization” provision, together with other safeguards [in Title III] constitutes the congressionally designed bulwark against conduct of authorized electronic surveillance in a manner that violates the constitutional guidelines announced in *Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United States*, 389 U.S. 347 (1967). . . . Together [the provisions of Title III] are intended to meet the test of the Constitution that electronic surveillance techniques be used only under the most precise and discriminate circumstances.⁸⁷

In other words, both Congress and at least some members of the Supreme Court explicitly viewed Title III’s minimization requirement as one of the necessary limits that rendered authorized wiretapping

the American Bar Association Standards for Criminal Justice, 66 OKLA. L. REV. 699, 720 (2014) (advocating further development of use restrictions). Professor Orin Kerr uses searches of computers as an example. He argues that the execution of warrants for select contents of an individual’s computer require protections beyond the warrant itself and that the Fourth Amendment should be interpreted to “impose a use restriction on nonresponsive data seized during the execution of computer warrants.” Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 1 (2015) (symposium keynote). He advocates, in other words, a two-step process where the acquisition stage imposes very few restrictions on the government, but the Fourth Amendment then steps in to limit what the government is allowed to do with that information. *Id.* The FISC reached a very similar result, albeit not through constitutional reasoning, with the bulk collection programs. *See infra* Section III.A.

86. 18 U.S.C. § 2518(5) (2012). *Berger* requires “[l]imitations on the officer executing the eavesdrop order which would (a) prevent his searching unauthorized areas, and (b) prevent further searching once the property sought is found.” S. REP. NO. 90-1097, at 74; *see also id.* at 75 (noting *Katz*’s observation that the surveillance at issue in that case would have been constitutionally valid had the government gotten a judicial order, at least in part because “the agents confined their surveillance to the brief periods during which petitioner used the telephone booth and took great care to overhear only the conversations of the petitioner himself”).

87. *Bynum v. United States*, 423 U.S. 952, 952 (1975) (Brennan, J., dissenting) (citing S. REP. NO. 90-1097, at 68); *see also Scott v. United States*, 425 U.S. 917, 917–18 (1976) (Brennan J., dissenting) (quoting *Bynum*, 423 U.S. at 952).

constitutional. Lower courts have reached this conclusion explicitly.⁸⁸ Title III may have been the first appearance of minimization requirements, but it would be far from the last.

2. *Foreign Intelligence Surveillance Act (FISA) minimization*

Whereas the need for Title III grew out of legal uncertainty about the constitutional limits of wiretapping, the need for FISA in the early 1970s was grounded in both legal uncertainty regarding wiretapping for foreign intelligence purposes and decades of troubling use of government surveillance. The legal uncertainty arose from the absence of congressional or judicial articulation of the constitutional requirements of surveillance for foreign intelligence purposes. In 1972, the Supreme Court in the *Keith* case⁸⁹ made clear that the First and Fourth Amendments demanded that intelligence collection to protect against *domestic* threats be subject to ex ante judicial approval,⁹⁰ but it expressly declined to determine whether such oversight was necessary when targeting foreign powers.⁹¹ *Keith* also raised the possibility that procedures used in approving domestic *intelligence collection* need not be identical to those used for *criminal investigations*.⁹² Title III also disclaimed applicability to *any* national-security-related intelligence collection.⁹³ And lower courts addressing the scope of the President's power to engage in warrantless foreign intelligence surveillance had reached inconsistent conclusions.⁹⁴

88. *In re Sealed Case*, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (citing *United States v. Falls*, 34 F.3d 674, 680 (8th Cir. 1994)) (noting that some circuit courts have held that minimization is a “constitutionally significant” element of Title III).

89. *United States v. U.S. Dist. Ct. for the E. Dist. of Mich.*, 407 U.S. 297 (1972) [hereinafter *Keith*].

90. *Id.* at 314–21, 323–24.

91. *Id.* at 308.

92. *Id.* at 322 (stating that the Court “recognize[d] that domestic security surveillance may involve different policy and practical considerations from the surveillance of ‘ordinary crime.’ . . . Given these potential distinctions . . . Congress may wish to consider protective standards for [intelligence surveillance] which differ from those” in Title III).

93. *Id.* at 302–06.

94. Compare *United States v. Butenko*, 494 F.2d 593, 604–05 (3d Cir. 1974) (en banc) (finding that warrantless electronic surveillance whose primary purpose is to obtain foreign intelligence information is lawful), and *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973) (“[T]he President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence.”), with *Zweibon v. Mitchell*, 516 F.2d 594, 636–59 (D.C. Cir.

Investigators therefore had no guidance regarding either the scope or the content of the warrant requirement when it came to foreign intelligence collection.

In the absence of legal clarity on this point—both before and after 1972—the executive branch for decades had assumed (over)broad authority to engage in unilateral electronic surveillance for the purposes of both domestic and foreign intelligence collection. The United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (known as the Church Committee for its chair, Senator Frank Church (D-ID)) revealed that from the 1930s through the 1970s, Democratic and Republican administrations alike had wiretapped and bugged American citizens without any judicial authorization.⁹⁵ In fact, surveillance ostensibly designed to gather “foreign intelligence” during the Cold War was used to eavesdrop on and harass Americans—including journalists, activists, and even members of Congress—who engaged in no criminal activity and who posed no genuine threat to the national security.”⁹⁶ A desire to curb these executive excesses and impose limits to prevent their recurrence was a motivating force behind FISA.⁹⁷

So while *Keith* exposed the need for congressional guidance regarding foreign intelligence surveillance rules, the Church

1975) (questioning whether a foreign intelligence exception to the warrant requirement would be constitutional).

95. See SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, BOOK II: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 12 (1976) [hereinafter CHURCH COMMITTEE BOOK II].

96. S. REP. NO. 95-604, at 8 (1977) (quoting CHURCH COMMITTEE BOOK II, *supra* note 95, at 12). Examples of the improper surveillance that took place during the Cold War in the absence of sufficient judicial oversight are legion. Perhaps most notorious was the FBI’s effort to “neutralize” Dr. Martin Luther King, Jr. CHURCH COMMITTEE BOOK II, *supra* note 95, at 11. The FBI employed electronic surveillance “to obtain information about the ‘private activities of Dr. King and his advisors’” in order to “completely discredit” him. *Id.* Many activist groups were also subject to warrantless surveillance—civil rights groups, members of the Women’s Liberation Movement, conservative Christian groups, anti-war student groups. *Id.* at 7, 105, 167. Initially targeted at thwarting communist subversion, see MARK V. TUSHNET, MAKING CIVIL RIGHTS LAW: THURGOOD MARSHALL AND THE SUPREME COURT, 1931–1961, at 295 (1994), this surveillance eventually became “purely political,” targeting people “on the basis of their political beliefs.” CHURCH COMMITTEE BOOK II, *supra* note 95, at 5, 118, 225.

97. S. REP. NO. 95-604, at 6–7 (FISA was “in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused”).

Committee documented why any statute authorizing foreign intelligence surveillance must include strict limitations as well. A recurring theme as members of Congress deliberated over the legislation that would ultimately become FISA was the need to balance foreign intelligence needs with privacy concerns.⁹⁸ Ultimately, the bill's drafters felt that its contents reflected "recognition by both the Executive Branch and the Congress that the statutory rule of law must prevail in the area of foreign intelligence surveillance" and that the lesson of "recent years" is that "such statutory safeguards" are a necessity.⁹⁹

As with Title III, FISA's procedural safeguards reflected Congress's reasoned opinion regarding what protections were necessary to render FISA constitutional. The legislation "embodies a legislative judgment that court orders and other procedural safeguards are necessary to insure [sic] that electronic surveillance by the U.S. Government within this country conforms to the fundamental principles of the [F]ourth [A]mendment."¹⁰⁰

Minimization procedures were an integral part of the procedural framework designed to keep FISA within the bounds of the Constitution. And while these procedures are generally meant "to parallel the minimization provision in" Title III, there are some critical differences.¹⁰¹ Foreign intelligence information is more difficult to isolate at acquisition because for "technological reasons, it may not be

98. See, e.g., *Foreign Intelligence Surveillance Act: Hearings on H.R. 7308 Before the Subcomm. on Courts, Civil Liberties & the Admin. of Justice of the H. Comm. on the Judiciary, 95th Cong. 80 (1978)* (statement of Sen. Edward Kennedy) (FISA was "designed to strike a balance, a careful balance, that will protect the security of the United States without infringing on the civil liberties and rights of the American people"); S. REP. NO. 95-604, at 3 (some amendments made to the bill over time were explicitly designed "to provide further safeguards for individuals subjected to electronic surveillance").

99. S. REP. NO. 95-604, at 7.

100. S. REP. NO. 95-701, at 13 (1978); *id.* at 9 (statement of need for the legislation); see also Laura K. Donohue, *supra* note 54, at 219-22 ("FISA was Congress's express decision to curb executive power as a constitutional matter.").

101. S. REP. NO. 95-701, at 39; see also H.R. REP. NO. 95-1283, at 54 (1978) (explaining that FISA minimization procedures will apply at the "acquisition, retention, and dissemination" stages); *supra* note 86 and accompanying text (showing that Title III minimization happens only at acquisition). Then-Attorney General Griffin Bell agreed that "the American people need the imposition of minimization standards" because there had been "too much dissemination . . . due to carelessness or without thinking." *Foreign Intelligence Surveillance Act of 1978: Hearings on S. 1566 Before the Subcomm. on Intelligence & the Rights of Ams. of the S. Select Comm. on Intelligence, 95th Cong. 24 (1978)*.

possible to avoid acquiring all conversations” from a particular facility, such as a particular phone line, rather than only those relevant to the court order.¹⁰² Another barrier to minimizing collection is that, “[g]iven the targets of FISA surveillance, it will often be the case that intercepted communications will be in code or a foreign language for which there is no contemporaneously available translator, and the activities of foreign agents will involve multiple actors and complex plots.”¹⁰³ So the government cannot be certain at the point of acquisition which communications have foreign intelligence value. Recognizing that effective minimization of acquisition “may be more difficult in the foreign intelligence area than in the more traditional criminal area,” the minimization procedures FISA placed on the *collection* of foreign intelligence were not as rigorous as those used in the criminal context.¹⁰⁴

To compensate for this initial permissiveness, Congress introduced in FISA the idea of minimizing not only collection, but also *retention* and *dissemination*. Because the government would be collecting more information under FISA than under Title III—some of it entirely unrelated to the investigation—there must be rules governing the use of that incidentally collected information.¹⁰⁵ In other words, because minimization of intelligence *collection* proves particularly challenging, minimization must limit *retention*, *use*, and *dissemination*.

102. S. REP. NO. 95-604, at 38.

103. *In re Sealed Case*, 310 F.3d 717, 741 (FISA Ct. Rev. 2002).

104. S. REP. NO. 94-1035, at 42 (1976); *see also* S. REP. NO. 95-604, at 52–53 (noting that “effective minimization may be more difficult in the foreign intelligence area than in the more traditional criminal area” and the bill therefore contains “less restrictive procedures” than the criminal wiretapping law); S. REP. NO. 95-701, at 58–59 (“[F]or example, 90 days . . . of surveillance per order rather than 30 days.”).

105. S. REP. NO. 95-701, at 17 (arguing that FISA would “provide adequate protection for Americans” by “strengthen[ing] the ‘minimization’ requirements to limit strictly the dissemination of information about U.S. persons”); *see also Foreign Intelligence Surveillance Act of 1978: Hearings on S. 1566 Before the Subcomm. on Intelligence & the Rights of Ams. of the S. Select Comm. on Intelligence*, 95th Cong. 220 (1978) (“[M]inimization procedures are a vital part of the bill because they regulate the acquisition, retention, and most importantly, the dissemination of information about U.S. persons who are . . . inadvertently swept up into the intelligence gathering process.”). The FISA definition of minimization procedures includes retention and dissemination minimization, requiring “information concerning American citizens and lawful resident aliens be handled in such a way as to assure that it is used only for the purposes specified in the definition and that it cannot be used for any other purpose.” S. REP. NO. 95-604, at 38; S. REP. NO. 95-701, at 41.

Congress's vision of FISA's minimization provisions included a strong and continuing role for the courts in overseeing both the procedures themselves and the government's compliance with them. As if to emphasize this point, FISA "spell[ed] out" in a separate provision "the judge's authority explicitly so that there [would] be no doubt that a judge may review the manner in which information about U.S. persons is being handled."¹⁰⁶ So a FISA judge "has the discretionary power to modify the order sought, such as with regard to . . . the minimization procedures to be followed."¹⁰⁷ In addition, Congress intended for the FISA Court to "give these [minimization] procedures most careful consideration. If it is not convinced that they will be effective, the application should be denied or the procedures modified."¹⁰⁸ Moreover, "the court shall monitor compliance with the minimization procedures" it imposes, and "[f]ailure to abide by the minimization procedures may be treated as contempt of court."¹⁰⁹

Courts immediately recognized the significance of minimization procedures. In upholding FISA against constitutional challenge, one federal appellate court, citing a Senate committee report, noted that "FISA reflects both Congress's 'legislative judgment' that the court orders and other procedural safeguards laid out in [FISA] 'are necessary to insure [sic] that electronic surveillance by the U.S. Government within this country conforms to the fundamental principles of the [F]ourth [A]mendment.'"¹¹⁰ The court agreed with Congress that the framework created in FISA was constitutionally sufficient: "We regard the procedures fashioned in FISA as a constitutionally adequate balancing of the individual's Fourth

106. S. REP. NO. 95-701, at 57; *see also* H.R. REP. NO. 95-1720, at 29 (1978) (FISA provides that "at the end of the period of time for which electronic surveillance was approved . . . the judge may assess compliance with the minimization procedures"); S. REP. NO. 95-701, at 41 ("[T]he judge, in approving the minimization procedures, could require specific restrictions on the retrieval of such information."); S. REP. NO. 95-604, at 38 (similar); 124 CONG. REC. 10,900 (1978) (statement of Sen. Evan Bayh, in support of an amendment (which was adopted) clarifying the judiciary's power to oversee the implementation of minimization procedures).

107. S. REP. NO. 95-604, at 47.

108. *Id.* at 48; *see also* Helene E. Schwartz, *Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs are Doing Their Jobs*, 12 RUTGERS L.J. 405, 439 (1981) (emphasizing the FISC's independent role in assessing the sufficiency of minimization procedures).

109. S. REP. NO. 95-604, at 49.

110. *United States v. Duggan*, 743 F.2d 59, 73 (2d Cir. 1984) (citing S. REP. NO. 95-701, at 13).

Amendment rights against the nation's need to obtain foreign intelligence information."¹¹¹ Implicit in both Congress' and the court's analysis of FISA's procedures is that any scheme *less* protective of individual rights risked being found insufficient from a constitutional standpoint.

So minimization procedures from their inception were designed as tools for judges to employ when the nature of the surveillance at issue rendered other procedural protections insufficient to protect individual privacy. As the next Part demonstrates, the FISA Court has increasingly relied upon minimization to shoulder the constitutional load as more traditional privacy protections have been reduced.

B. Foreign Intelligence Minimization Evolves

The drafters of FISA never could have predicted the ways in which surveillance programs—and the FISA Court's role in administering them—would expand after 9/11.¹¹² Nor could they have imagined the advances in the government's technological power to collect and analyze large volumes of information. This Section shows how the FISA Court's use of minimization evolved alongside ever-expanding government surveillance authority. As the government's powers increased, the court employed more and more rigorous minimization procedures to shore up the defense of constitutional values. This evolution began with the passage of FISA itself—discussed above and studied in more detail in Section II.B.1—whose minimization provision is much more robust than the minimization contemplated for criminal wiretaps. Section II.B.2 continues with the introduction of the FISA Amendments Act regime. Because that regime eliminates several aspects of traditional privacy protections, the FISA Court's constitutional analysis relies in large part on the ability of minimization procedures to serve as a sufficient substitute for those protections.¹¹³ Section II.B.3 then shows how minimization's evolution culminated with the post-9/11 bulk collection regimes. When it came to those

111. *Id.* at 73; *see also id.* at 74 (“We conclude that these requirements [including minimization procedures] provide an appropriate balance between the individual's interest in privacy and the government's need to obtain foreign intelligence information . . .”).

112. For an in-depth discussion of the FISA Court's job description and its post-9/11 evolution, see Emily Berman, *The Two Faces of the Foreign Intelligence Surveillance Court*, 91 *IND. L.J.* 1191 (2016).

113. The FISA Amendments Act is codified beginning at 50 U.S.C. § 1801.

programs, the FISA Court turned to minimization to fill the gaps in privacy protections, despite the absence of constitutional necessity.

1. Step one: Traditional FISA minimization

All of FISA's procedural safeguards, including minimization, are analogs of the requirements necessary to obtain a criminal wiretapping warrant under Title III. To be sure, the *Keith* Court noted differences between criminal and intelligence investigations and invited Congress to design an approval process that reflected those differences.¹¹⁴ And Congress did take the court up on its suggestion. Nevertheless, while not identical, FISA's privacy protections parallel those of Title III.¹¹⁵

First, FISA orders must be issued prior to the surveillance by a neutral magistrate—a FISA judge.¹¹⁶ Second, FISA orders for electronic surveillance and physical searches require a probable cause showing. While Title III warrants require “probable cause for belief that an individual is committing, has committed, or is about to commit” a crime,¹¹⁷ FISA warrants for electronic surveillance require that the government establish probable cause that “the target of the electronic surveillance is a foreign power or an agent of a foreign power.”¹¹⁸ So while both statutes have probable cause requirements, the nature of the requisite probable cause is different and FISA's is an easier standard to meet. Third, like Title III, FISA includes particularity requirements. As an initial matter, an executive branch official must designate the *type* of foreign intelligence information being sought.¹¹⁹ The government's application also must provide “the identity, if known, or a description of the target” of the surveillance.¹²⁰

114. *See supra* note 92.

115. *In re Sealed Case*, 310 F.3d 717, 737 (FISA Ct. Rev. 2002).

116. 50 U.S.C. § 1805(a) (2012). There are some emergency exceptions allowing the government to apply for a FISA Court order after having initiated surveillance. 50 U.S.C. § 1805(3).

117. 18 U.S.C. § 2518(3)(a) (2012).

118. 50 U.S.C. § 1805(a)(2)(A). A U.S. person (a citizen or legal permanent resident) meets the definition of “[a]gent of a foreign power” only when she may be engaged in criminal activity on behalf of a foreign power, such as espionage. § 1801(b)(2)(A).

119. 50 U.S.C. § 1804(a)(6)(D), (E). “Foreign intelligence information” can be information to protect against an attack, sabotage, or espionage, information that relates to “the national defense or the security of the United States,” or information related to U.S. foreign affairs. 50 U.S.C. § 1801(e).

120. 50 U.S.C. § 1804(a)(2).

So when a FISA Court judge issues an order for the collection of electronic communications—i.e., phone calls and emails—that order includes the “identity . . . or a description of the specific target,” “the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known,” “the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance,” “the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance,” and “the period of time during which the electronic surveillance is approved.”¹²¹

Just as *Berger* prompted Congress to include a handful of protections beyond those required for ordinary search warrants in Title III, FISA’s drafters included analogous provisions, including minimization.¹²² When it comes to minimization, FISA adds additional elements not present in Title III. Congress and the courts have accepted that acquisition minimization in the intelligence context is of necessity more permissive. As a result, FISA “centers on an expanded conception of minimization,”¹²³ requiring minimization not only of what is acquired but also what is retained and disseminated.¹²⁴ Thus, both Congress and the courts have recognized that in reducing the protections generated by Title III’s strict probable cause and acquisition minimization requirements, effective retention and dissemination minimization becomes a necessary counterweight.

121. 50 U.S.C. § 1805(c).

122. Recall that the warrant requirement of the Fourth Amendment includes three essential elements: (1) warrants issued by a neutral magistrate, (2) a showing of probable cause and (3) particularity. *See supra* note 17 and accompanying text. When FISA’s additional procedures are compared with those of Title III, FISA requires more robust protections for some and more permissive ones for others. *In re Sealed Case*, 310 F.3d 717, 741 (FISA Ct. Rev. 2002) (noting that FISA permits less minimization during acquisition). Both statutes require that the information be unavailable through other investigative procedures, 50 U.S.C. § 1804(a)(6)(C), 18 U.S.C. § 2518(3)(c), and both have duration provisions, 50 U.S.C. § 1805(d)(1) (90 days), 18 U.S.C. § 2518(5) (30 days). FISA’s longer duration limit is justified by “the nature of national security surveillance, which is ‘often long range and involves the interrelation of various sources and types of information.’” *In re Sealed Case*, 310 F.3d at 740 (citations omitted).

123. *United States v. Belfield*, 692 F.2d 141, 148 (D.C. Cir. 1982); *see also United States v. Cavanaugh*, 807 F.2d 787, 788–89 (9th Cir. 1987) (noting that a FISA order was constitutional because the application established the requisite probable cause and included minimization procedures).

124. *In re Sealed Case*, 310 F.3d at 740.

According to the FISA Court of Review (FISCR), a court that hears appeals from decisions of FISA judges, the elements of FISA that mirror traditional warrant requirements and Title III protections are integral to the statute's constitutionality. In fact, "the more a set of procedures resembles those associated with the traditional warrant requirements, the more easily it can be determined that those procedures are within constitutional bounds."¹²⁵ The FISCR held that FISA remained constitutional despite changes to statutory language enacted in the USA PATRIOT Act,¹²⁶ at least in part, because the statutes' rules retained the requirements of a neutral magistrate, probable cause, and particularity as well as necessity, duration, and minimization.¹²⁷ For purposes of this Article, I take no position regarding the constitutionality of FISA; I only point out that where Title III rules were more stringent—i.e. more aggressive acquisition minimization—FISA used enhanced minimization procedures to compensate.

So when it comes to FISA, minimization procedures—in particular at the retention and dissemination phases—have always been an integral part of the regime and central to its constitutionality. As surveillance programs have added to the government's collection authority, minimization procedures become even more central to securing judicial approval. Ultimately, the FISC comes to use minimization to limit government surveillance powers even in contexts where the Constitution (arguably) does not require such limits. The balance of this Section will explore this evolution.

2. *Step two: The FISA amendments act minimization*

The types of surveillance authorized by FISA—and hence the jurisdiction of the FISA Court—has expanded since the statute's enactment in 1978. The most significant modification came as a result

125. *In re Directives* [REDACTED] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1013 (FISA Ct. Rev. 2008); *see also In re Sealed Case*, 310 F.3d at 742 ("We do not decide the issue but note that to the extent a FISA order comes close to meeting Title III, that certainly bears on its reasonableness under the Fourth Amendment.").

126. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 274 (2001).

127. *In re Sealed Case*, 310 F.3d at 740. Note that despite its procedural elements, some argue that FISA itself fails to meet Fourth Amendment requirements. This Article takes no position on the constitutionality of any particular surveillance statute.

of two statutes—first the temporary Protect America Act (PAA)¹²⁸ and then the FISA Amendments Act (FAA).¹²⁹ The role of minimization as a constitutional stop-gap becomes evident with the PAA and the FAA. These statutes authorize the government to engage in what has always been viewed as the most intrusive form of surveillance—the collection of communications content. The PAA expired after six months,¹³⁰ but it was replaced by the nearly identical FAA, which remains in force. Both the PAA and the FAA authorized electronic surveillance of non-U.S. person targets “reasonably believed to be located outside the United States” when the government seeks foreign intelligence information from those people.¹³¹ Collection under this authority is sometimes referred to as either section 702 collection (for the section of the FAA that codified the power) or as PRISM, the NSA’s code word for collection under section 702.

The structure of the FAA regime departs from previous electronic surveillance rules in significant ways. The most obvious is the treatment of the usual probable cause and particularity requirements. Under the FAA, the government need not establish probable cause of anything to initiate surveillance.¹³² And the only particularity requirements that the government must meet are premised on geography and motivation—if a target is reasonably believed to be outside the United States (and is not a U.S. person) and the purpose of the surveillance is to collect foreign intelligence information, the statute is satisfied.¹³³

Another major departure from typical Fourth Amendment protections is the modified role of the FISA judge. Under the FAA, the FISC is not asked to determine whether the government has met the statutory requirements. In other words, the court does not consider whether the government has sufficiently demonstrated that a proposed target satisfies the statutory targeting rules. In fact, no neutral magistrate ever assesses whether an individual target meets the

128. Protect America Act, Pub. L. No. 110–55, § 105B, 121 Stat. 552, 552 (2007).

129. FISA Amendments Act, Pub. L. No. 110–261, 122 Stat. 2436 (codified at 50 U.S.C. §§ 1881a–1885c).

130. Protect America Act, § 6(c) (imposing a 180-day sunset provision).

131. 50 U.S.C. § 1881a(g)(2).

132. 50 U.S.C. § 1881a(d) (limiting targeting requirements to geographic considerations rather than individualized suspicion).

133. 50 U.S.C. § 1881a(a).

statutory targeting requirements. Instead, the FISC's ex ante role is confined to reviewing the executive branch's internal rules for targeting and minimization and deciding whether those rules, when used by executive branch officials, are sufficiently likely to yield targets and protect information in ways that comply with the statute's requirements.¹³⁴

Thus, the PAA and FAA purport to dispense with all of the traditional warrant requirements. Despite these innovations, the FISC found that the surveillance authorized in the PAA (a holding almost certainly applicable to the FAA as well) satisfies constitutional demands.¹³⁵ In so holding, however, the court did not simply provide a stamp of approval for surveillance lacking the types of protections deemed indispensable by the Supreme Court and Congress in the past.

In determining that the PAA regime satisfied the Fourth Amendment's reasonableness requirement, the court looked outside the statutory regime for means of compensating for the fact that traditional safeguards have gone by the wayside. A critical observation that the court made early in its analysis is that the surveillance orders at issue "require certain protections *above and beyond those specified by the PAA.*"¹³⁶ So while the PAA itself dispenses with cause, particularity, and ex ante review requirements, the court declines to consider whether the PAA's statutory requirements, without more, are sufficient to render the provision constitutional. Instead, the court looked at the particular orders challenged in this case, including the additional protections that the FISC had included when initially issuing those orders.

These extra-statutory restrictions play a critical role in the court's analysis. First, the court points to the fact that the surveillance orders incorporate procedures from Executive Order 12333, which "allay[s] the probable cause concern," according to the court, because it means that the Attorney General "had to make a determination that probable cause existed to believe that the targeted person is a foreign power or

134. 50 U.S.C. § 1881a(i)(2). Some argue that this difference arguably renders the regime unconstitutional. See generally Donohue, *supra* note 54 (challenging the FAA's constitutionality). A challenge to the constitutionality of the FAA, *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), was dismissed for lack of standing.

135. *In re Directives* [REDACTED] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1016 (FISA Ct. Rev. 2008).

136. *Id.* at 1007 (emphasis added).

an agent of a foreign power.”¹³⁷ Second, when it comes to particularity, the court asserts that the government’s “pre-surveillance” targeting procedures are “analogous to and in conformity with the particularity showing contemplated” by FISA.¹³⁸ These procedures, the court determines, “[w]hen combined with the PAA’s other protections,” provide “constitutionally sufficient compensation” for any alleged procedural deficiencies.¹³⁹ So in the absence of statutory probable cause and particularity requirements, the court imports them from other sources. And while these additional sources were not specifically labeled minimization procedures in the FISCR’s opinion, that is what they are: a set of extra-statutory rules imposed by the FISA Court to compensate for the fact that the statute itself lacks sufficient constitutional protection for the contents of communications.

As with previous statutes authorizing electronic surveillance, the particularity and probable cause requirements are insufficient. This is especially so here, where those requirements are implemented by the government itself, rather than the FISC. The FISCR therefore turns to minimization procedures as “an additional backstop against . . . errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons.”¹⁴⁰ Given the applicable procedures, the FISCR concluded that they were sufficient because in addition to requiring “a showing of particularity” and “a meaningful probable cause determination,”¹⁴¹ they also require that “effective minimization procedures are in place.”¹⁴² Thus, any privacy concerns raised by permitting the government to make its own probable cause and particularity determinations rather than

137. *Id.* at 1014.

138. *Id.* at 1013–14. This assessment is impossible to confirm as those targeting procedures are not public. The FAA’s (the PAA’s successor statute) targeting procedures, however, were released in the wake of the Edward Snowden leaks. Those procedures lay out how the NSA will attempt to identify the location of the target, assess whether the target qualifies as a U.S. person or not, and determine whether the target possesses or is likely to communicate foreign intelligence information. Eric H. Holder, Jr., Att’y Gen., *Exhibit A: Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended*, at 1–4 (2009), <https://ia601709.us.archive.org/0/items/2007NSAProceduresUsedToTargetNonUSPersons/exhibit-a.pdf>.

139. *In re Directives*, 551 F.3d at 1014.

140. *Id.* at 1015.

141. *Id.* at 1016.

142. *Id.* at 1015.

submitting these determinations to a neutral magistrate, the court seems to say, will be mitigated by minimization procedures. So the court relies upon minimization to mitigate any increased error rate attributable to the elimination of the traditional forms of Fourth Amendment protection. When it comes to bulk collection, this phenomenon becomes even more pronounced.

3. Step three: Bulk collection minimization

While FISA essentially dispensed with efforts to implement minimization procedures at acquisition, bulk collection authorizations go a step further, eliminating even the minimal probable cause and targeting particularity requirements in FISA and the FAA. As a result, we see FISC judges relying *exclusively* on minimization procedures to impose constraints on the government. This Subsection discusses the FISC's creative use of minimization in the context of three bulk collection programs. The first collects the content of communications, material at the heart of Fourth Amendment protection and is the subject of Section II.B.3.a. The other two programs—the bulk collection of telephony and Internet metadata, detailed in Section I.A.—collect only metadata. As the FISC does not consider these programs subject to constitutional limitations,¹⁴³ you might expect it to impose permissive minimization procedures, or even none at all. In fact, as Section II.B.3.b demonstrates, the opposite proves true. Rather than dispense with the inconvenience of minimization procedures because the Constitution does not require them, the court imposes relatively burdensome limits on the retention, use, and dissemination of metadata collected in bulk. While this deployment of minimization rules may at first seem inexplicable, a close reading of the FISA Court's orders and the government's applications suggests an explanation, to which I will turn in Part III.

a. Minimization and section 702 upstream collection. One telling example of minimization's outsized role in bulk collection programs came in response to a government application for reauthorization of its section 702 upstream collection authority. Section 702, whose name refers to the section of the FAA that authorizes the collection,¹⁴⁴

143. See *supra* Section I.B.

144. See 50 U.S.C. § 1881a.

771 *Quasi-Constitutional Protections and Government Surveillance*

targets non-U.S. persons abroad through the “tasking” of “selectors.”¹⁴⁵ A “selector” is “a specific communications facility . . . used by the target, such as the target’s email address or telephone number” (key words, such as “terrorism” or “ISIS,” cannot be selectors) that is expected to “yield foreign intelligence information.”¹⁴⁶ “[T]asking” a selector is merely the process of identifying it as one whose communications should be captured.¹⁴⁷ “Thus, in the terminology of section 702, people (non-U.S. persons reasonably believed to be located outside the United States) are *targeted*; selectors (e.g., email addresses, telephone numbers) are *tasked*.”¹⁴⁸

Even though “upstream” collection—like the section 702 PRISM program¹⁴⁹—is targeted at particular selectors, in actual operation it collects communications beyond those authorized by the FAA. Upstream collection of Internet communications acquires data by using selectors—such as email addresses and IP addresses—associated with particular targets to capture information directly from the Internet “backbone” as it transits the web.¹⁵⁰ Upstream collection wanders into bulk collection territory, however, due to two technological challenges associated with Internet communications. The first is that upstream collection cannot be limited to Internet communications that are only to and/or from a tasked selector. Instead, it will also capture communications “in which the tasked selector is referenced within the acquired [communication], but the

145. PCLOB SECTION 702 REPORT, *supra* note 16, at 41–42.

146. *Id.* at 32–33, 135.

147. *Id.* at 7, 21.

148. *Id.* at 32.

149. Recall that PRISM is simply the implementation of the FAA regime in which the government seeks electronic communications associated with particular accounts from service providers after having determined that the account-holder is a non-U.S. person located outside the United States whose communications are a source of foreign intelligence information. 50 U.S.C. § 1881a. The government rather than the FISC decides which selectors to task, but collection is limited to the communications of those chosen selectors. *See supra* notes 133–134 and accompanying text.

150. *E.g.*, James Bamford, *They Know Much More Than You Think*, N.Y. REV. OF BOOKS (Aug. 15, 2013) (quoting NSA slide describing upstream collection as “collection of communications on fiber cables and infrastructure as data flows past”). The NSA also collects the contents of telephone calls via upstream collection, but unlike the upstream Internet data collection, it does not result in the collection of communications to/from non-targets. PCLOB SECTION 702 REPORT, *supra* note 16, at 36.

target is not necessarily a participant in the communication”—so-called “about” collection.¹⁵¹ So when it comes to Internet communications, upstream collection nets *all* communications that are to, from, *or* about tasked selectors.¹⁵² A communication sent from one innocent U.S. person to another (neither of whom is a surveillance target), but which includes somewhere in the message a tasked email address, will be captured in upstream collection.

The second technological hurdle is the fact that information moves across the Internet in the form of transactions. “An Internet transaction” is “any set of data that travels across the Internet together such that it may be understood by a device on the Internet.”¹⁵³ Some transactions—known as multiple-communications transactions (MCTs)—contain within them multiple discrete communications.¹⁵⁴ NSA’s upstream Internet collection devices, however, cannot “distinguish[] between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications.”¹⁵⁵ Nor can the NSA “identify the parties to any particular communication within a transaction” prior to collection.¹⁵⁶ As a result, if an MCT includes at least one communication to, from, or about a tasked selector, the NSA will acquire the *entire* MCT, even if the other communications within it are purely domestic and have nothing to do with a selector.¹⁵⁷ This means that some unpredictable number of entirely domestic communications that are not to, from, *or* about a target of surveillance

151. PCLOB SECTION 702 REPORT, *supra* note 16, at 37. Whether “about” collection is a valid use of section 702 authority is a matter of debate. *See, e.g.*, Donohue, *supra* note 54, at 253; Dia Kayyali, *The Way the NSA Uses Section 702 is Deeply Troubling. Here’s Why*, EFF BLOG (May 8, 2014, 5:10 PM), <https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why>; JAMEEL JAFFER, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD: PUBLIC HEARING ON SECTION 702 OF THE FISA AMENDMENTS ACT 21–24 (2014), https://www.aclu.org/sites/default/files/assets/pcllob_fisa_sect_702_hearing_-_jameel_jaffer_testimony_-_3-19-14.pdf.

152. PCLOB SECTION 702 REPORT, *supra* note 16, at 37.

153. *Id.* at 39.

154. *Id.*

155. *In re* [REDACTED], No. PR/TT [REDACTED], at 31 (FISA Ct. Oct. 3, 2011).

156. *Id.* at 43.

157. PCLOB SECTION 702 REPORT, *supra* note 16, at 39.

will be swept up in the upstream collection.¹⁵⁸ Personal communications of U.S. persons who have not been targeted are inevitably acquired. Upstream collection thus in some ways resembles bulk surveillance, even though the NSA is using selectors connected with specific targets.

In light of these realities, the FISC assessed the sufficiency of the NSA's upstream collection program's minimization procedures. Because "it is not feasible for NSA to limit its collection only to the relevant portion" of each transaction, the FISC determined that the existing minimization procedures as applied to acquisition were sufficient;¹⁵⁹ the court also found the NSA's dissemination minimization procedures acceptable.¹⁶⁰ When it came to retention, however, the court concluded that NSA's proposed handling of transactions containing wholly domestic communications tended to *maximize*—rather than minimize—the retention of information "not relevant to the authorized purpose of the acquisition."¹⁶¹ The deficiencies in the retention minimization rules thus rendered the collection unlawful under the FAA statute and unconstitutional under the Fourth Amendment.¹⁶²

The FISC's response was not to order the unconstitutional upstream program to cease operations. Instead, as Congress did with

158. *In re* [REDACTED], No. PR/TT [REDACTED], at 32–36 (FISA Ct. Oct. 3, 2011). Because the Internet automatically moves transactions in the most efficient way, a U.S.-based user "may send a communication (intentionally or otherwise) via a foreign server even if the intended recipient is also in the United States." PCLOB SECTION 702 REPORT, *supra* note 16, at 38. An NSA review of a random sample of 50,040 Internet transactions taken from the more than 13.25 million Internet transactions acquired through NSA's upstream collection during a six-month period showed that the "NSA acquires approximately 2,000-10,000 [Internet transactions] each year that contain at least one wholly domestic communication." *In re* [REDACTED], at 33, 33 n.30 (emphasis in the original); *see also id.* at 50 n.45 ("[U]ntil NSA's manual review of a six-month sample of its upstream collection revealed the acquisition of wholly domestic communications, the government asserted that NSA had never found a wholly domestic communication in its upstream collection."). The FISC found that "NSA is likely acquiring tens of thousands of discrete communications of non-target United States persons and persons in the United States" simply because "their communications are included in [a transaction] selected for acquisition by NSA's upstream collection devices." *Id.* at 37.

159. *Id.* at 57–58.

160. *Id.* at 66–67.

161. *Id.* at 59, 78 (NSA's minimization procedures enhanced "the risk of error, overretention [sic], and dissemination of non-target information, including information protected by the Fourth Amendment").

162. *Id.*

FISA in 1978¹⁶³ and the FISC did in *In re Directives*,¹⁶⁴ the FISC turned to amplified minimization to compensate for inevitable over-collection. The government adopted a series of new minimization procedures focused specifically on retention and dissemination of domestic communications incidentally collected through the NSA's upstream collection program.¹⁶⁵ The court subsequently determined that these additional safeguards—procedures to identify, segregate, and limit the use of information “not relevant to the authorized purpose of the acquisition”—rendered the program statutorily and constitutionally sound.¹⁶⁶ A FISA judge thus employed enhanced minimization procedures to transform an unconstitutional collection program into one that complied with both statutory and Fourth Amendment requirements.

b. Minimization and bulk metadata collection. Recall that the government got FISA Court approval to engage in two bulk metadata collection programs. The first used an expansive interpretation of FISA's pen/trap provision to acquire Internet metadata about American's electronic communications, especially emails.¹⁶⁷ The second program used a similarly aggressive interpretation of section 215 of the USA PATRIOT Act, also known as the FISA “business records provision,”¹⁶⁸ to collect in bulk domestic telephony metadata—including telephone numbers dialed and the date, time, and duration of the call.¹⁶⁹ The NSA could query the resulting databases using seed identifiers (usually phone numbers or email addresses) and analyze the results of the queries through contact

163. *See supra* Section II.A.2.

164. *See supra* note 135–142 and accompanying text.

165. *In re* [REDACTED], No. PR/TT [REDACTED], Memorandum Opinion, at 7–11 (FISA Ct. Nov. 30, 2011) (explaining that the additional minimization procedures had “three main elements: (1) the post-acquisition segregation of those types of transactions that are most likely to contain non-target information concerning United States persons or persons in the United States; (2) special handling and marking requirements for transactions that have been removed from or that are not subject to segregation; and (3) a two-year default retention period for all upstream acquisitions”).

166. *Id.* at 14.

167. *See supra* notes 29–32 and accompanying text; 50 U.S.C. § 1842 (2012).

168. *See supra* notes 35–42 and accompanying text; 50 U.S.C. § 1861.

169. *See supra* note 39 and accompanying text.

chaining to identify individuals with as-yet-undiscovered terrorist connections.¹⁷⁰

Recall also that despite the government and the FISC's insistence on the inapplicability of the Constitution to the information collected by these programs, the FISC's orders exhibit a decided solicitude for the very same interests with which the Fourth Amendment is concerned—individual privacy and freedom from arbitrary government intrusions.¹⁷¹ The court did approve the programs, but only after imposing minimization procedures clearly focused on these quasi-constitutional privacy concerns. Notably, this was the case not only for the section 215 program (for which minimization was statutorily required) but also for the pen/trap provision, which did not include a statutory minimization requirement.¹⁷²

(1) *Bulk Internet metadata collection program minimization.* The application of minimization procedures to the collection of bulk Internet metadata is curious. Unlike upstream collection of communications content under section 702 of the FAA and some business records orders issued under section 215, pen/trap devices will never collect anything other than communications metadata—i.e., non-content information that is unprotected by the Fourth Amendment.¹⁷³ The statutory scheme reflected these characteristics in that the pen/trap provision lacked a statutory minimization requirement. In other words, neither the Constitution nor the relevant statute required the application of minimization procedures to metadata collected by pen/traps.

Despite the lack of a constitutional or statutory imperative to do so, the FISC imposed strict procedural protections on the bulk collection of Internet metadata. It did so because the “proposed

170. See *supra* Section I.B, I.C.

171. See *supra* Section I.C. and accompanying text.

172. This discrepancy arises out of the third-party doctrine. See *supra* Section I.B. Some tangible things that the government might seek under section 215—a personal diary, for example—will enjoy full Fourth Amendment protection. Since section 215 contemplates collection of some fully protected information as well as information—metadata, for example—that might be subject to the third-party doctrine, the statute requires minimization to ensure limits on the collection of any constitutional protected material. The pen/trap provision, by contrast, will only ever give the government access to communications metadata. Because the collection of communications metadata, in the government's view, cannot implicate Fourth Amendment concerns, minimization procedures were unnecessary.

173. FISC's Pen/Trap Opinion, *supra* note 25, at 18–19.

collection involves an extraordinarily broad implementation of a type of surveillance that Congress has regulated by statute even in its conventional, more narrowly targeted form.”¹⁷⁴ So the court employs a laundry list of restrictions—the description of which takes up the final seven pages of the FISC’s Pen/Trap Opinion—to mitigate the kinds of concerns that *would* arise if the Fourth Amendment *did* apply.¹⁷⁵ And while the opinion does not specifically identify these procedures as minimization procedures, they are all aimed at regulating the retention, use, and dissemination of U.S. person information—the very role that minimization procedures were created to play. In fact, these protections are nearly identical to the procedures later imposed on bulk telephony collection under the auspices of “minimization.”¹⁷⁶

Given the FISC’s clear discomfort with authorizing bulk surveillance despite the unprotected status of metadata, it is impossible to see these minimization procedures as anything other than a means of addressing the court’s constitutional—or quasi-constitutional—concerns.¹⁷⁷ In other words, the FISC recognizes—either consciously or unconsciously—that this particular use of the pen/trap authority raises privacy concerns that cannot be ignored. So while the use of minimization (or minimization-like) procedures for the Internet metadata program initially seems inexplicable, it is this instinct—that

174. FISC’s Pen/Trap Opinion, *supra* note 25, at 69, 80–87. The court then sums up this analysis: “[T]he bulk collection proposed in this case is analogous to suspicionless searches or seizures that have been upheld under the Fourth Amendment in that the Government’s need is compelling and immediate, the intrusion on individual privacy interests is limited, and bulk collection appears to be a reasonably effective means of detecting and monitoring [redacted] related operatives” *Id.* at 54. As a result, the FISC finds the information is relevant even though “only a very small proportion of the huge volume of information collected will be *directly* relevant.” *Id.* (emphasis added).

175. These restrictions can be attributed, in part, to the court’s concern that the program threatened to abridge the First Amendment rights of innocent persons. The court therefore devoted “further attention” to the First Amendment issues raised by the government’s application in hopes of finding ways to narrow the scope of the government intrusion. FISC’s Pen/Trap Opinion, *supra* note 25, at 3 n.3, 56. The court pressed the government on how long the data would retain operational value, *id.* at 3 n.3, and asked First-Amendment related questions, *id.* Ultimately, this inquiry led the court to mandate that no email address “believed to be used by a U.S. person” could be “regarded as associated with [a terrorist organization] solely on the basis of activities that are protected by the First Amendment to the Constitution.” *Id.* at 83–84.

176. *See infra* Section II.B.3.

177. *See supra* Section I.C.

government collection of bulk metadata implicates the same constitutional values protected by minimization in other FISA provisions—that animates the FISC’s Pen/Trap Opinion’s use of such procedures. Faced with the quasi-constitutional implications of the program, the FISC simply employed its usual mechanism for plugging constitutionally impermissible privacy holes in surveillance law minimization.

Those restrictions represented a wide array of measures, many of which the government proposed in its application; others were added by the FISA judge.¹⁷⁸ Some were purely procedural: Access to the metadata was limited to authorized analysts by requiring a user name and password, records of which would be maintained for auditing purposes;¹⁷⁹ all data queries had to be approved by one of a limited number of senior officials;¹⁸⁰ and the information collected under this program would be available for querying for only 18 months, after which it must be transferred to “off-line” storage accessible only by a cleared administrator, and then destroyed 18 months later.¹⁸¹ The order also includes a ninety-day limit on the length of the authorized surveillance.¹⁸² When applying for reauthorization of that authority, the FISC required the government to include a report discussing the queries that had been made since the previous application and describing any proposed changes.¹⁸³

There were also more substantive elements. First, the court imposed the Reasonable Articulate Suspicion (RAS) standard. Under this standard, before querying the database regarding any specific seed, the NSA had to conclude

178. *E.g.*, Memorandum of Law and Fact in Support of Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes at 3, *In re* [REDACTED] (FISA Ct. 2004) (No. PR/TT); FISC’s Pen/Trap Opinion, *supra* note 25, at 69–70 n.50 (“The principal changes that the Court has made from the procedures described in the application are the inclusion of a ‘First Amendment proviso’ as part of the ‘reasonable suspicion’ standard for an [redacted] to be used as the basis for querying archives meta data, . . . the adoption of a date after which meta data may not be retained, . . . and an enhanced role for the NSA’s Office of General Counsel in the implementation of this authority . . .”).

179. FISC’s Pen/Trap Opinion, *supra* note 25, at 83.

180. *Id.* at 84.

181. *Id.* at 85–86.

182. *Id.* at 80.

183. *Id.* at 86–87.

based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known [redacted—probably email or IP address] is associated with [redacted—probably international terrorist organization or Al Qaeda] *provided, however, that an* [redacted—likely email or IP address again] *believed to be used by a U.S. person shall not be regarded as associated with* [redacted—probably international terrorist organization or Al Qaeda again] *solely on the basis of activities that are protected by the First Amendment to the Constitution.*¹⁸⁴

The FISC assigned to the NSA's Office of General Counsel the job of ensuring that analysts with access to the metadata received adequate training, monitoring compliance with the RAS standard, and reviewing the legal adequacy of the basis of any query using a seed account used by a U.S. person.¹⁸⁵

There were also restrictions on the permissible use of the information collected. Analysis of the information was limited to "contact chaining" and one additional redacted process.¹⁸⁶ Dissemination of U.S. person information was strictly limited and had to comply with the presidential directive laying out minimization procedures applicable within the executive branch.¹⁸⁷

So long as the government program satisfied the statutory requirements and was consistent with the Constitution—two findings the FISA judge clearly made—it should have been lawful *without* adding any of these additional parameters. As we know, minimization procedures are usually a means of ensuring that surveillance methods remain within the scope of Fourth Amendment limits; it follows that no such procedures are required when the statute does not require them and the Fourth Amendment does not apply. The FISC, however,

184. *Id.* at 57–58.

185. *Id.* at 85.

186. *Id.* at 83.

187. *Id.* at 85; *see also* NSA, United States Signals Intelligence Directive SP0018, Legal Compliance and U.S. Persons Minimization Procedures § 7.2(c) (Jan. 25, 2011) (requiring that before U.S. person information can be disseminated outside the NSA, a high-level NSA official has to determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand [that] counterterrorism information or assess its importance).

771 *Quasi-Constitutional Protections and Government Surveillance*

imposed a substantial list of mechanisms seemingly aimed at protecting U.S. persons' quasi-constitutional right to privacy.¹⁸⁸ So despite the purported absence of constitutional or statutory minimization requirements, minimization requirements were imposed.

(2) *Bulk telephony metadata collection program minimization.*

The bulk collection program under section 215 also collected only metadata. Both the government and the FISC also declared the Fourth Amendment inapplicable. Unlike the pen/trap provision at the time, however, section 215 *did* include statutory minimization requirements. It is therefore no surprise that the FISC included such requirements in its orders authorizing the bulk collection of telephony metadata. Minimization procedures, however, are not a one-size-fits-all proposition. Instead, they can be “reasonably designed in light of the purpose and technique of an order.”¹⁸⁹ Minimization procedures regarding the information found in a diary or a laptop computer, for example, might demand more stringent minimization procedures than those necessary for non-content information. Since some of the tangible things collected pursuant to section 215 would enjoy Fourth Amendment protection, the statute must include a minimization requirement. When it comes to telephony metadata, however, it seems that the minimization procedures required for the unprotected bulk telephony metadata would be minimal. Yet, like the Internet metadata collection program, the FISC imposes a laundry list of rigorous minimization procedures on the telephony bulk collection program. In fact, the FISC used as a model the rules laid down in the 2004

188. This instinct was vindicated when the USA Freedom Act added a requirement for “[p]rivacy procedures” to the most recent version of the FISA pen/trap provision. 50 U.S.C.A. § 1842(h) (Westlaw through Pub. L. No. 114-219).

189. 50 U.S.C. § 1861(g)(2)(A) (2012).

Internet metadata opinion,¹⁹⁰ including, for example, the same RAS standard for querying the database and similar limits on access.¹⁹¹

Once the FISC approved the pen/trap and section 215 bulk collection programs, the evolution of minimization was complete. The idea began in conjunction with Title III, a constitutional bolster to the requirements applicable to traditional criminal warrants. It was expanded in FISA, recognizing that fewer limits on acquisition required additional controls over retention, use, and dissemination. The PAA and FAA represented a sea change, eliminating individualized showings to a FISA judge, instead allowing the FISC to approve or disapprove of targeting and minimization procedures, but leaving all actual targeting decisions with the government. As a result, the FISCR found itself both turning to a new sort of extra-statutory limitations and relying more heavily on traditional minimization procedures to guard against unauthorized surveillance. Finally, in the upstream section 702 collection and the section 215 and pen/trap programs, all traditional *ex ante* warrant requirements are abandoned. Yet, even in circumstances where the information at issue is arguably not protected by the Constitution and the statute does not require it, the court insisted on including rigorous

190. Unless otherwise specified, I refer to the original minimization procedures imposed on the programs. Over time, the FISA Court imposed additional internal oversight controls. Once every 90-day authorization period, the Justice Department had to review a sample of the NSA's justifications for querying data; periodically, the NSA's Inspector General, General Counsel, and Signals Intelligence Directorate Oversight and Compliance Office had to review the program; and twice every 90 days, the NSA's Office of General Counsel (subsequently substituted with the Justice Department's National Security Division) conducted random spot checks to ensure the NSA was collecting only authorized material. *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [REDACTED], BR 06-05, at 6–10 (FISA Ct. Aug. 18, 2006). The first and third of these requirements were added to the Internet metadata collection orders in 2009 after the FISC was made aware of a number of instances of government non-compliance. Beginning at that time, the NSA had to submit periodic reports to the FISC regarding both the queries it had conducted and the information it had disseminated. *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 09-13, Order Regarding Further Compliance Incidents, at 3 (FISA Ct. Sept. 25, 2009). The Justice Department's National Security Division was also given a greater role in assessing the adequacy of training and compliance. *Id.* And RAS findings regarding particular seeds were time-limited—the NSA could not query in perpetuity using a seed that had once satisfied the RAS standard. *Id.* As these modifications were introduced to the telephony metadata program, parallel measures were imposed on the pen/trap program. *In re* [REDACTED], No. PR/TT [REDACTED], at 8 n.10 (FISA Ct. 2010).

191. There were some differences. For example, telephony metadata could be retained for a longer period of time (five years) than Internet metadata (three years).

minimization procedures in its orders. The next Part offers an explanation of why the FISC acted as it did.

III. QUASI-CONSTITUTIONAL RIGHTS: MINIMIZATION AS FOURTH AMENDMENT SUBSTITUTE

From the criminal wiretaps authorized by the 1968 Title III statute to post-9/11 bulk metadata collection, courts have consistently pointed to minimization as a critical procedural protection. As I argued in Part II, this has been especially true when other procedural protections were statutorily weakened or removed entirely. In those circumstances, minimization became one of the few remaining privacy-protection tools available to the FISC. This Part explores the court's creative application of minimization in bulk metadata collection in more detail.

Section A argues that the FISA Court employed minimization procedures to incorporate approximations of the traditional Fourth Amendment protections—*ex ante* review, targeting based on cause, and particularity—into programs that fundamentally (and by design) lacked these features. In this way, the court was able to reclaim via minimization procedures some of the privacy-protection territory lost to the third-party doctrine.

Even if one agrees with this characterization of the court's opinions, questions persist: If the bulk collection programs raised sufficient constitutional concerns that the court believed it needed to replicate constitutional protections, why did it work so hard to fit the square peg of bulk collection into the round hole of traditional privacy-protection principles? The court simply could have rejected the government's applications as inconsistent with the applicable statutes or the Constitution.¹⁹² Similarly, if neither the Constitution nor the applicable statutes demanded the minimization procedures the court imposed, why did the government agree to comply with them?

Section B ventures to suggest answers—or at least partial answers—to some of these questions. It argues that the FISC's response to government applications for bulk collection authority was a rational decision if viewed from an institutional perspective. As we

192. As the court's critics have demonstrated, there were ample arguments available to a court wanting to take that path. *See, e.g.*, PCLOB SECTION 215 REPORT, *supra* note 5, at 67–102 (laying out numerous arguments that the program was not authorized by section 215); Donohue, *supra* note 5, at 836–96 (same); Donohue, *supra* note 54, at 202–62 (same).

have seen, the court harbored real misgivings about the constitutionality of some aspects of these programs. At the same time, the urgency with which the government pressed for the programs' approval indicated that a flat-out judicial denial of authority would *not* be warmly received by the executive branch. Yet, the executive did crave the court's seal of approval. So rather than force a constitutional confrontation, the court engaged the government in a negotiation. The price it demanded for its stamp of legitimacy was government compliance with procedures designed to protect constitutional values. It thus simultaneously sought to protect quasi-constitutional rights, claim some measure of oversight power, even (or maybe especially) in the context of bulk collection, and yet let the government implement its desired program.

A. Approximating the Fourth Amendment Through Minimization

Recall that the three fundamental elements of the warrant requirement are the following: ex ante review by a neutral decision maker, a showing of cause to that decision maker, and a particularized explanation of the goal of the search or seizure. This Section looks at the minimization requirements imposed by the FISC in the bulk collection context through the lens of these traditional warrant requirements. It illustrates how FISA Court judges imposed approximations of those traditional requirements in order to constrain the government's use of data collected in bulk in ways designed to protect quasi-constitutional privacy rights.¹⁹³

193. It is worth noting that the FISA Court is far from the first to employ quasi-constitutional reasoning. Indeed, there are a variety of contexts in which courts have engaged in an elucidation of constitutional *principles* without declaring specific constitutional *demands*. One such circumstance is the use of so-called prophylactic rules. A prophylactic rule is designed to safeguard a particular constitutional right—or cluster of rights—by barring state conduct that may not itself actually violate the substance of the Constitution. *See generally* Mitchell Berman, *Constitutional Decision Rules*, 90 VA. L. REV. 1 (2004); Henry P. Monaghan, *Foreword: Constitutional Common Law*, 89 HARV. L. REV. 1 (1975); David A. Strauss, *The Ubiquity of Prophylactic Rules*, 55 U. CHI. L. REV. 190 (1988) (noting that prophylactic rules are “a central and necessary feature of constitutional law”). Such rules draw the line of permissible government action “beyond the Constitution’s strict requirements in order to ensure that constitutional values receive effective vindication in practice.” Richard Fallon Jr., *Judicially Manageable Standards and Constitutional Meaning*, 119 HARV. L. REV. 1275, 1304 (2006). The prophylactic rule, in other words, admittedly protects rights beyond the scope of the relevant constitutional provision. The exclusionary rule, which requires the suppression of evidence collected in violation of the Fourth Amendment, provides an example. *Mapp v. Ohio*, 367 U.S.

1. Prior approval

The FISC approximated the first, an independent ex ante review in the context of the bulk collection programs, in several ways. First, the FISC made clear that the court itself had no intention of ceding its own independent oversight role, however circumscribed it might be in the bulk collection context. To secure a FISA Court order under either the pen/trap or section 215 provisions, the government must submit a certification attesting that the requested surveillance authority will likely produce foreign intelligence information or is relevant to an ongoing investigation into terrorism or espionage.¹⁹⁴ When the government argued that “FISA prohibits the Court from engaging in any substantive review” of the certifications that the government included in its application, the court rejected that interpretation.¹⁹⁵ The statutory language seemed to support the government’s claim that the FISC had the power to ensure that the government provided the necessary certification, but not to review that certification for accuracy or adequacy.¹⁹⁶ Despite this language,

643 (1961) (exclusionary rule applies to the states); *Weeks v. United States*, 232 U.S. 383 (1914) (exclusionary rule applies to the federal government). No one would argue that the exclusionary rule is a part of the substantive rights protected by the Fourth Amendment. Instead, it is a deterrent to law enforcement misconduct designed to protect those substantive rights. *United States v. Calandra*, 414 U.S. 338, 347 (1974) (noting that “the rule’s prime purpose is to deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment”). In requiring the exclusionary rule, the Supreme Court identified and (over?)protected the actual constitutional rights that were at stake—the Fourth Amendment’s right to privacy and freedom from unreasonable government intrusion—but announced a decision that did not require the court to define the scope of those rights with any specificity. In the seminal article about prophylactic rules, Professor Henry Monaghan identified *Miranda v. Arizona*, 384 U.S. 436 (1966), as another example. See Monaghan, *supra*, at 21–22. That case famously required that for confessions elicited during custodial interrogations to be admissible in court, law enforcement officials must read the suspect his so-called *Miranda* warnings. 384 U.S. at 444–45. At the time Monaghan was writing, the Supreme Court maintained that *Miranda* warnings were *not* constitutionally required by the Fifth Amendment. See, e.g., *Oregon v. Elstad*, 470 U.S. 298, 306 (1985); *New York v. Quarles*, 467 U.S. 649, 657 (1984); *Michigan v. Tucker*, 417 U.S. 433, 443–45 (1974). They were instead a judge-made form of over-enforcement of Fifth Amendment rights against self-incrimination. See Monaghan, *supra*, at 21. While the Supreme Court ultimately rejected this view of *Miranda* warnings, holding in *United States v. Dickerson*, 530 U.S. 428 (2000), that the Fifth Amendment did in fact require those warnings, there are other instances of the phenomenon that remain on the books.

194. 50 U.S.C. § 1842(c)(2) (2012) (pen/trap); § 1861(b)(2)(A) (section 215).

195. FISC’s Pen/Trap Opinion, *supra* note 25, at 26.

196. 50 U.S.C. § 1861(c)(1) (“Upon an application made pursuant to this section, if the judge finds that the application meets [all of the statutory requirements], the judge shall enter

the court concluded that “authorizing the Court to issue an order when a certification is made, and requiring it to do so without resolving doubts about the correctness of the certification, are quite different.”¹⁹⁷ So while the nature of bulk collection does not afford the FISC a role to assess cause and particularity for each individual surveillance target, the court nevertheless insisted on retaining the ex ante power to question the sufficiency of the government’s application and the adequacy of its planned means of implementation.

Second, the FISC imposed multiple minimization rules on the use of metadata *already collected* that approximate ex ante search approval. With a bulk collection program, there are no targeting decisions made prior to collection. But the FISC imposed limits on the use and dissemination of the data, ensuring at least some ex ante review before the data that had been amassed was accessed by humans. In both the Internet and telephony metadata context, the FISC required approval by one of a handful of high-level NSA officers before a query of the metadata database could be initiated.¹⁹⁸ And when the query involved “seed accounts used by U.S. persons,” the court went a step further, requiring an ex ante determination from the NSA’s Office of General Counsel (“NSA OGC”) that each such query met the required RAS standard.¹⁹⁹ So while individual determinations regarding whose metadata would be accessed did not require *judicial* approval, no query could be undertaken without sign-off from an internal executive branch watchdog. Thus, a high-level official knowledgeable about the law had to determine that the relevant legal standards—standards set by the court in its minimization requirements (e.g., the RAS standard for queries)—were met. To be sure, executive branch officials are not independent magistrates. But someone in the NSA’s OGC is more likely to make a neutral assessment than an analyst seeking intelligence. Involving that office therefore promoted individual privacy interests.

an ex parte order as requested.”); 50 U.S.C. § 1842(d)(1) (“Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested . . . if the judge finds that the application satisfies the requirements of this section.”).

197. FISC’s Pen/Trap Opinion, *supra* note 25, at 26–27 n.19.

198. *Id.* at 84.

199. *Id.* at 84–85; *see also id.* at 85 n.58 (“[I]t shall be incumbent on NSA’s Office of General Counsel to review the legal adequacy for the basis of such queries.”); *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [REDACTED], BR 06-05, at 6 (FISA Ct. Aug. 18, 2006). The NSA’s Office of the General Counsel also was assigned the role of ensuring that analysts allowed to access the data had sufficient training with respect to the RAS standard. FISC’s Pen/Trap Opinion, *supra* note 25, at 84.

The court's minimization rules also required periodic review to ensure that the ex ante protections it set up were working properly. Pursuant to the FISA Court's order, the Justice Department reviewed a sample of the NSA's bulk database queries every ninety days to check whether the NSA's justifications for querying the data met the RAS standard. Similarly, the NSA OGC was required to conduct random spot checks twice every ninety days to ensure the program was complying with legal and policy requirements (this responsibility was later transferred to the Justice Department's National Security Division). In addition, before the court would renew the program for another ninety-day period, the government was required to submit to the FISC a "report discussing the queries that have been made" and "the NSA's application of the [RAS] standard" since the last application.²⁰⁰ When the court discovered—in part through these oversight mechanisms—that the NSA was failing to comply with existing rules, it added additional tools to track the NSA's performance in this regard. For a brief period, the court reverted to the traditional form of ex ante review for queries of telephony metadata database: for several months it required the government to seek FISC approval of each specific query before that query could be initiated.²⁰¹ This minimization procedure remained in place until the FISC was satisfied that the internal procedures had been modified so as to be effective.²⁰²

Of course, these measures are not themselves ex ante review mechanisms, but they do permit the FISC to monitor whether the ex ante procedures set out in its orders were adequately filtering queries. This information gave the FISC an ongoing role in ensuring that the

200. FISC's Pen/Trap Opinion, *supra* note 25, at 86.

201. *In re* Production of Tangible Things from [REDACTED], Order, No. BR 08-13, at 18–19 (FISA Ct. Mar. 2, 2009); Donohue, *supra* note 5, at 817–19. This process was the one subsequently codified in the USA Freedom Act. That statute retains the RAS standard, and assigns to the FISC the determination whether the standard has been met with respect to each particular seed. USA Freedom Act, § 101(a)(3)(c)(i). Other enhanced minimization procedures were imposed as well. For example, the FISC began requiring periodic reports regarding both queries and dissemination of metadata collected through both bulk collection programs. *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [REDACTED] BR: 09-06, at 7–8 (FISA Ct. Mar. June 22, 2009).

202. *In re* Production of Tangible Things from [REDACTED], Order, No. BR 08-13, at 18–19 (FISA Ct. Mar. 2, 2009)

government was complying with the *ex ante* requirements the court had imposed.

2. *Cause*

None of these pre-query review procedures would have had any meaning if there were no substantive standards that the government was required to meet. The bulk collection minimization procedures imposed such a standard in the form of the RAS standard. Recall that the government could query the information in the bulk databases only after determining that there was reasonable articulable suspicion that the particular phone number, email address, or other seed to be tasked was related to international terrorism.²⁰³ This standard is, in essence, a cause requirement. Before conducting a search, the government must have some individualized suspicion regarding the seed whose information it seeks to obtain.

It is clear that the FISC itself viewed the RAS standard as a cause requirement. When setting out the rules for how the RAS must be applied to the Internet metadata, the court recognized that conventional, individual pen/trap surveillance includes judicial review of cause before any collection takes place. “In this case,” the court asserts, “the *analogous* decision to use a particular e-mail account as a seed account takes place [after collection].”²⁰⁴ The RAS standard according to the FISC, “will realize more fully the Government’s suggestion that “[t]he information actually viewed by any human being . . . will be just as limited—and will be based on the same targeted, individual standards—as in the case of an ordinary pen register or trap and trace device.”²⁰⁵ When it approved the bulk telephony collection program, the court imposed the same RAS requirement on queries of that data.²⁰⁶

To be sure, the standard is not probable cause, but it mirrors the cause requirements imposed on the pen/trap and section 215

203. FISC’s Pen/Trap Opinion, *supra* note 25, at 42, 57–80.

204. *Id.* at 85 n.58 (emphasis added) (contrasting traditional surveillance, where review of targeting decisions takes place before the government collects any information, with the bulk metadata program, where the government amasses a database before determining which seeds to query).

205. *Id.* at 58 n.41 (quoting a letter from the government).

206. *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [REDACTED], BR 06-05, at 4–5 (FISA Ct. Aug. 18, 2006).

771 *Quasi-Constitutional Protections and Government Surveillance*

collection authorities. Neither of those statutes authorized capture of the content of electronic communications, so they did not require the government to show probable cause before targeting a particular individual. Instead, they required “that the information likely to be obtained [was] foreign intelligence information . . . relevant to an ongoing investigation” into “international terrorism or clandestine intelligence activities.”²⁰⁷ The minimization procedures required at the query stage in the bulk collection context are no more forgiving than the pre-collection showing required to secure a similar order targeting a single individual. The difference comes in the timing of the cause showing—whether it is before or after the government acquires the metadata.

3. Particularity

When it comes to particularity, the bulk collection programs are a bit of a contradiction. On the one hand, collection is not directed at any particularized target; that is the point of the program. So, there is no particularity of collection at all in that regard. On the other hand, the purpose of the collection and the use of the information once acquired are subject to several particularity limitations analogous to those imposed on more targeted surveillance. Title III, for example, requires the government to designate “a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates,”²⁰⁸ while FISA requires an executive branch official to certify that the information sought is foreign intelligence information and to designate what type of foreign intelligence information is being sought.²⁰⁹ When it comes to bulk collection, similar particularity restrictions apply. The FISC limited the pen/trap collection program to Internet metadata “reasonably likely to identify the sources or destinations of the electronic communications” of known members of terrorist organizations.²¹⁰

207. 50 U.S.C. § 1842(c)(2) (2012) (pen/trap); *see also* § 1861(b)(2)(A) (requiring, under section 215, for an application to show that “the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities”).

208. 18 U.S.C. § 2518(4)(c) (2012).

209. 50 U.S.C. § 1804(a)(6) (A), (D)–(E).

210. FISC’s Pen/Trap Opinion, *supra* note 25, at 81.

And with respect to the telephone metadata, the statutory provision permits the collection of “any tangible thing,” but the bulk collection program was limited to “call detail records” that would help to identify unknown terrorists.²¹¹

The certainty that collection targeted in that way will collect a huge amount of irrelevant data might render that type of particularity relatively meaningless; additional particularity limits apply, however, *after* the information has been collected. Under the applicable minimization rules, queries of the data, for example, must be directed at particular seed identifiers.²¹² This means that humans will access only metadata related to individuals for whom there is a reasonable, articulable suspicion that their communications are relevant to an ongoing investigation. In the Internet metadata program, the government was limited to analyzing the information returned by a query in just one of two ways: contact chaining or some additional process, the nature of which remains redacted.²¹³ So the nature of the information collected and, more significantly, the requirements for initiating queries, is automatically particularized as part of the goal of the bulk collection programs.

The court’s minimization requirements do not implement the Fourth Amendment protections that normally apply to the collection of communications content. But they do create proxies for each of those traditional protections. Thus, rather than merely allowing bulk collection to go forward with few or no limits (as the Constitution and statutes arguably allowed), the FISA Court employed minimization rules to impose limitations that took Fourth Amendment concerns into account—all to protect quasi-constitutional privacy rights.

211. Exhibit C: Memorandum of Law in Support of Application for Certain Tangible Things for Investigations to Protect Against International Terrorism at 2, *In re* [REDACTED] (FISA Ct. May 23, 2006) (No. [REDACTED]). Title III and FISA also require information about the nature and location of facilities where the surveillance will be directed, who is authorized to intercept the information, and the means by which the information will be collected. All of these variables are also evident in the description of the bulk collection programs themselves. They authorize the NSA to target certain telephone or Internet communications facilities through its technological tools designed to do so. *See supra* Section I.A.

212. *See supra* Section III.A.2.

213. FISC’s Pen/Trap Opinion, *supra* note 25, at 83.

B. Explaining the FISA Court's Use of Minimization in Bulk Metadata Collection Programs

This section suggests an explanation for the FISA Court's treatment of bulk collection programs grounded in an institutional perspective. On the one hand, the FISA judges were not unaware of the threats to individual privacy that the bulk collection programs represented; they clearly did not feel comfortable simply ignoring the threat to constitutional values posed by the programs. At the same time, they harbored no illusions about their own ability to successfully prevent the executive from implementing the programs. Moreover, they likely entertained their own security-based doubts about the prudence of attempting to do so. Seeing constitutional questions lurking while simultaneously doubting the wisdom of addressing them directly, the FISC's use of minimization tells a story not of a court out of its depth or abdicating its oversight responsibilities,²¹⁴ but of a court working hard to impose meaningful limits on the government and retain for itself some oversight power. Indeed, it may be that the limits set out by the FISC were the most stringent the judges felt empowered to impose.²¹⁵ This Section will explore the forces at work on a court in the FISC's situation, making the case that what the court actually did is allow the surveillance to go forward, but only after extracting from the government an agreement to abide by minimization rules that served to protect quasi-constitutional privacy rights.

1. The FISA Court's strategic deference

It is well established that courts do not operate in a vacuum.²¹⁶ Social science research has definitively shown that in their decision making, judges "take into account the preferences and likely actions of other relevant actors," such as "their colleagues," courts that might review their decisions, and "members of the other branches of

214. *See supra* note 5 (collecting critiques of the FISC's performance).

215. The FISA Court's critics may be correct that the limits the court imposed were insufficient to satisfy statutory or constitutional requirements. *See* sources cited *supra* note 5. This paper does not take a position on that question. Rather, it seeks to offer an alternative interpretation of the FISA Court's performance.

216. *See* Lee Epstein & Tonja Jacobi, *The Strategic Analysis of Judicial Decisions*, 6 ANN. REV. L. & SOC. SCI. 341, 342 (2010).

government.”²¹⁷ Theories of strategic judging assume that judges do not want to see their decisions reversed, want to see their decisions complied with, and do not want to invoke retaliation from Congress or the executive branch.²¹⁸ To render decisions that others “will respect and with which they will comply,” a “judge must attend to the preferences and likely actions”²¹⁹ of those institutions that “could override or otherwise thwart their decisions.”²²⁰ After all, it may be the judiciary that renders judgments, but those judgments are left to the executive to enforce.²²¹ Any judge considering issuing a decision that it fears the executive branch might not enforce will think twice before issuing that mandate. As every first year law student learns, the genius of Chief Justice John Marshall in *Marbury v. Madison* is that he established the power of judicial review without provoking a confrontation with the Jefferson Administration—a confrontation the court was sure to lose.²²²

While it was certainly within the FISA Court’s purview to withhold judicial authorization for bulk collection, there is reason to believe the FISC might have questioned whether the executive would acquiesce in such a decision. One reason for such skepticism was the government’s repeated emphasis on the pressing need to use bulk surveillance to fight the threat of terrorism. Consider the 2006 application for the bulk collection of telephony metadata. The government’s memo in support of its application emphasized the

217. *Id.*

218. *See id.* at 344, 350–51.

219. *Id.* at 344.

220. *Id.* at 351.

221. John O. McGinnis, *Constitutional Review by the Executive in Foreign Affairs and War Powers: A Consequence of Rational Choice in the Separation of Powers*, 56 L. & CONTEMP. PROBS. 293, 301 (1993). As President Jackson famously (and likely apocryphally) responded to an opinion by Chief Justice Marshall declaring invalid Georgia’s seizure of Native American land on which gold had been found, “John Marshall has made his decision, now let him enforce it.” *See, e.g.*, Justice Stephen Breyer, Assoc. Justice, Supreme Court of the U.S., Boston College Law School Commencement Remarks (May 23, 2003), https://www.supremecourt.gov/publicinfo/speeches/viewsspeech/sp_05-23-03. Regardless of whether Jackson actually spoke those words, he did proceed to ignore the Court’s decision. *See id.*

222. *Marbury v. Madison*, 5 U.S. (1 Cranch) 137 (1803).

threat.²²³ Several pages of the brief was devoted to a section labeled “The Al Qaeda Threat,” which includes a detailed description of the 9/11 attacks, an event about which no American who lived through the day would need reminding.²²⁴ It went on to detail Al Qaeda’s previous attacks on U.S. interests, such as the bombing of the U.S.S. Cole, the embassy bombings in East Africa in 1998, and its continuing desire to strike at America.²²⁵ It raised the specter of Osama bin Laden (who at the time remained at large), describing his post-9/11 audio recordings; and it referred to intelligence community concerns that the next attack in the United States “might use chemical, biological, radiological, or nuclear weapons”—not based on any specific threat information but instead on Al Qaeda’s desire to develop such capability.²²⁶ This part of the government’s brief concludes by asserting that “the proposed request for . . . [telephone] records would greatly help the United States prevent another such catastrophic terrorist attack, one that [redacted—presumably Al Qaeda] itself has claimed would be larger than the attacks of September 11th.”²²⁷ That section comes, moreover, immediately following the introduction. In other words, before making its legal argument as to why the bulk telephony metadata collection was consistent with the FISA and the Fourth Amendment, the government first ensured that the FISC judge reviewing the application had in mind the tragic events of 9/11 and the specter of an even more tragic subsequent attack.

The 2004 brief supporting the government’s application for the initial pen register/trap and trace authorization for bulk Internet collection likely began in exactly the same way. It is impossible to be sure, however, as the first several pages of the publicly available version of that document are redacted.²²⁸ We do know for certain that the full-court press was not limited to the government’s written submissions.

223. Exhibit C: Memorandum of Law in Support of Application for Certain Tangible Things for Investigations to Protect Against International Terrorism at 4–7, [REDACTED] (FISA Ct. [REDACTED]) (No. BR: 06-05).

224. *Id.*

225. *Id.* at 5–7.

226. *Id.* at 7.

227. *Id.*

228. Memorandum of Law in Support of Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes at 1, 5–9, [REDACTED] (FISA Ct. [REDACTED]) (No. PR/TT).

In addition to reading the government's brief, "the court was briefed on the pressing need for this [Internet metadata] . . . by, among others, the Attorney General, the Director of Central Intelligence, the Director of the FBI, the Director of the NSA, the Counsel to the President, the Assistant Attorney General for the Office of Legal Counsel, the Director of the Terrorist Threat Integration Center . . . , and the Counsel for Intelligence Policy."²²⁹ The not-so-subtle message delivered by the government's arguments supporting its applications for bulk collection authority—whether intentionally or not—is that, without it, America will be vulnerable to a significant terrorist threat, there is no other means by which such a program can be authorized, and any judge who denies the government the tools it needs to combat that threat will be responsible for the resulting harm.²³⁰ While this message may have reflected the executive's sincerely held belief, it could not help but impact judicial decision making.

The government continued to play this card throughout the life of the bulk collection programs. In 2009, for example, the FISA Court had discovered the government's failure to abide by the minimization procedures that had been part of the court's prior orders.²³¹ The government's transgressions, according to the FISC, "[o]rdinarily" would have provided "sufficient grounds for a FISC judge to deny the [government's reauthorization] application."²³² "[G]iven the government's repeated representations that the [bulk] collection

229. Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes at 4, [REDACTED] (FISA Ct. [REDACTED]) (No. PR/TT [REDACTED]); *see also In re* [REDACTED], No. PR/TT [REDACTED], Opinion and Order, at 27 (FISA Ct. [REDACTED]) ("[T]he government has provided a detailed explanation of 1) the threat currently posed by [redacted], 2) the reasons the bulk collection described in the application is believed necessary as a means for NSA [redacted], and 3) how that information will contribute to FBI investigations to protect against [redacted]"); *id.* at 31–35 (supplying another, redacted description of the threat).

230. Reluctance to place obstacles in front of counterterrorism policymakers is a well-worn theme of national security oversight challenges. *See, e.g.*, CHARLIE SAVAGE, POWER WARS: INSIDE OBAMA'S POST-9/11 PRESIDENCY 183 (2015) ("Officials who try to stop [a national security program that is up and running] put themselves in a difficult position, in terms of career risk and blame avoidance"); Emily Berman, *Regulating Domestic Intelligence Collection*, 71 WASH. & LEE L. REV. 3 (2014); Emily Berman, *The Paradox of Counterterrorism Sunset Provisions*, 81 FORDHAM L. REV. 1777 (2013).

231. *E.g.*, *In re* Production of Tangible Things from [REDACTED], No. BR 08-13, Order, at 12 (FISA Ct. Mar. 2, 2009).

232. *Id.*

771 *Quasi-Constitutional Protections and Government Surveillance*

of . . . [phone records] [wa]s vital to national security,” however, “the Court conclude[d] it would not be prudent to order that the government’s acquisition . . . cease at this time.”²³³ So the fact that the government averred that the program was critical to national security convinced the FISC to approve a reauthorization application that it might ordinarily have denied.

In addition, the government undermined the FISC’s ability to throw the ball back into Congress’s lap. A court’s usual response to an executive plea for unlawful powers is to deny the powers and allow Congress to confer them legislatively if it chooses to do so. Here, however, the government argued that the FISC needed to interpret FISA expansively because if the FISC denied the authority, the intelligence community could not ask Congress to expand the statute. To do so, they argued, would compromise the security (i.e., secrecy) of the program.²³⁴ So rejecting the government’s application would not simply force the executive to go back to Congress to ask for expanded authority. It would, in effect, preclude entirely the use of this purportedly indispensable tool.

Any doubt the FISC might have had about the government’s willingness to abide by adverse FISC decisions would have been reinforced by the fact that the government had proved itself willing to initiate these types of programs *without* judicial approval. Shortly after 9/11, for example, the executive branch implemented a series of programs entirely free of judicial oversight to collect the content of and metadata about electronic communications of targets suspected to have a connection with al Qaeda, known as the President’s Surveillance Program (PSP).²³⁵ Even the FISA statute’s explicit statement that its procedures were the “exclusive means” of engaging in electronic surveillance did not prevent the implementation of the

233. *Id.* at 17–18.

234. Memorandum of Law and Fact in Support of Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes at 61, [REDACTED] (FISA Ct. 2004) (No. PR/TT [REDACTED]).

235. OFFICE OF THE INSPECTOR GEN. OF THE DEP’T OF DEF., ET AL., UNCLASSIFIED REPORT ON THE PRESIDENT’S SURVEILLANCE PROGRAM 1 (2009); *see also* OFFICE OF THE INSPECTOR GEN. OF THE DEP’T OF JUSTICE, A REVIEW OF THE DEPARTMENT OF JUSTICE’S INVOLVEMENT WITH THE PRESIDENT’S SURVEILLANCE PROGRAM 255 (2009) (quoting then-White House Counsel Alberto Gonzales as responding to one FISA court opinion denying a particularly aggressive interpretation of FISA by saying that the denial “confirmed our concern about going to the FISA Court”).

PSP.²³⁶ Aspects of this unilateral executive branch surveillance continued even after the *New York Times* revealed the telephone content portion of the program in 2005.²³⁷ The government applications to the FISC for bulk collection authority were, in fact, part of the process of migrating what had been unilateral executive programs into ones supervised by the FISA court.²³⁸ FISA judges would therefore not be unreasonable in worrying that a FISC rejection may be just as likely to prompt the government to achieve its ends through extrajudicial means as it would be to prevent the collection of metadata in bulk.

And even if the FISC was confident its decision—whatever it was—would be respected, there were other strategic reasons to defer to the executive. It is no secret that in wartime or times of crisis, courts reviewing alleged infringements on individual liberties exhibit significant deference to executive branch positions.²³⁹ One explanation is courts' reluctance to make an independent determination regarding the efficacy of executive-branch national security programs—especially given their access to only incomplete information.²⁴⁰ The FISC was no different; its opinions explicitly state that the judges considered themselves ill-equipped to evaluate the potential costs of denying authorization for the bulk metadata programs or to determine independently their value more generally.²⁴¹ Instead, they take as a given the government's argument that the proposed collection is both necessary to protect against domestic terrorist threats and effective in doing so.²⁴² If the court accepted as true the government's strident

236. 18 U.S.C. § 2511(2)(f) (2000 & Supp. III 2003).

237. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 15, 2005, at A1.

238. See *infra* Section II.B.2.

239. The academic literature on this point is extensive. See, e.g., CLINTON ROSSITER, THE SUPREME COURT AND THE COMMANDER IN CHIEF (1976); Lee Epstein et al., *The Supreme Court During Crisis: How War Affects Only Non-War Cases*, 80 N.Y.U. L. REV. 1 (2005); David Cole, *Judging the Next Emergency: Judicial Review and Individual Rights in Times of Crisis*, 101 MICH. L. REV. 2565 (2003); Oren Gross, *Chaos and Rules: Should Responses to Violent Crises Always be Constitutional?*, 112 YALE L.J. 1011 (2003); see also Cole, *supra*, at 2570–71 (listing various reasons for judicial deference to the executive in times of crisis).

240. E.g., Cole, *supra* note 239, at 2570.

241. See FISC's Pen/Trap Opinion, *supra* note 25, at 48, 53.

242. *Id.* at 53 (“A low percentage of positive outcomes among the total number of searches or seizures does not necessarily render a program ineffective.”); *id.* at 53–54 (“[S]enior responsible officials, whose judgment on these matters is entitled to deference, . . . have

assurances about the necessity of the programs, the programs' privacy costs would have had to be high indeed to outweigh their security benefits.²⁴³ Another explanation is that members of the judiciary are not immune to the fear of terrorist attacks that permeates society at large. It may be that the government's arguments convinced the FISC that the program was necessary for America's safety. Or it may simply be that the FISC did not want to assume responsibility for any security consequences that might flow from shutting down the program. But whether it was fear of being cut out of the oversight loop entirely, aversion to denying the government a potentially valuable counterterrorism tool, or a refusal to have the blame for any future attack laid at its feet, the FISC was in no position to draw a line in the sand. As the next section explains, what the court did instead was eschew insistence on traditional Fourth Amendment procedural protections in favor of striking a bargain with the executive branch. The substance of that bargain was that the FISC would hold that the bulk collection programs were lawful and the government would abide by minimization rules that protected quasi-constitutional rights.

articulated why they believe that bulk collection and archiving of meta data are necessary to identify and monitor [redacted] operatives whose Internet communications would otherwise go undetected in the huge streams of [redacted].”).

243. As it turns out, perhaps the court should have exhibited less deference on this point. After the bulk collection programs became public, Congress refused to renew that authority unless the executive could demonstrate the value of the surveillance. It was unable to make such a showing. *See, e.g.*, MARSHALL ERWIN, HOOVER INST., *CONNECTING THE DOTS: ANALYSIS OF THE EFFECTIVENESS OF BULK PHONE RECORDS COLLECTION 2* (2015) (“[A]n analysis of the facts demonstrates that the bulk phone records collection program is of marginal value.”); PETER BERGEN ET AL., NEW AM. FOUND., *DO NSA’S BULK COLLECTION PROGRAMS STOP TERRORISTS?* (2014) (reaching same conclusion). In retrospect it is tempting to view this conclusion as further reason why the FISA Court never should have acquiesced to begin with. But lacking such information at the time it was faced with the decision, the FISC had little choice but to accept the government's assurances of the program's value. And as time went on and the FISC adjusted minimization requirements in response to executive branch compliance problems, the court did ultimately insist that the executive provide to the court an assessment of the value of allowing the bulk collection to continue. *In re* Production of Tangible Things From [REDACTED], No. BR 08-13, Order, at 13 (FISA Ct. Mar. 2, 2009) (“The time has come for the government to describe to the Court how, based on the information collected and analyzed during that time, the value of the program to the nation's security justifies the continued collection and retention of massive quantities of U.S. person information.”).

2. *The FISA Court's quasi-constitutional rulemaking*

Inter-branch bargaining is not uncommon. James Madison expected that the branches would check one another with their ambition;²⁴⁴ but it turns out that rather than compete with one another, the branches often shape separation of powers structures “through bargains and accommodation to advance their mutual institutional interests.”²⁴⁵ There is no reason to expect that government institutions would not engage in the same give and take on a more granular level. Just as different branches of government have different interests and competencies as a general matter, each will also have particular interests when it comes to individual interactions (or series of reactions). Here, the FISC negotiated with the executive over the scope of judicial review of bulk collection programs.

It takes two, of course, to bargain. Even accepting that the FISC wants to impose minimization procedures beyond what FISA or the Constitution requires, why would the government agree to abide by them? The answer is that the government benefited from the FISC's approach to bulk collection at least as much as the court did. Debates over the lawfulness of using the Internet bulk collection program *without* FISA Court approval had generated significant conflict within the executive branch.²⁴⁶ In fact, several high-level Justice Department officials had threatened to resign if changes were not made to address these legal concerns.²⁴⁷ To put this controversy to rest, the Justice Department's solution was to bring the program within the purview of the FISA Court. It was thus imperative for the Department of Justice to secure the court's stamp of approval for the program. In order to do so, the government had no choice but to strike a bargain with the FISA Court that included acceding to its insistence on extensive minimization procedures.

As a practical matter, FISA applications always involve what amounts to informal negotiation between the government and the court. The process is an iterative one, in which the presiding judge,

244. THE FEDERALIST NO. 51 (James Madison).

245. McGinnis, *supra* note 221, at 295–99; *see also* Aziz Z. Huq, *The Negotiated Structural Constitution*, 114 COLUM. L. REV. 1595 (2014).

246. OFFICE OF THE INSPECTOR GEN. OF THE DEP'T OF JUSTICE, *supra* note 218, at 99–129.

247. *Id.*

members of the FISA Court staff, and government lawyers responsible for preparing applications engage in a dialogue. In trying to bring the PSP's warrantless content collection within the purview of the FISA Court before Congress passed the PAA or FAA, for example, the Justice Department first provided for the FISC's consideration of a draft of its proposed legal argument during the court's semi-annual meeting.²⁴⁸ In the course of considering each individual application, a judge might insist on additional information from the government, require a hearing on a particular issue of fact or law, modify the government's proposed order, or impose additional conditions or limitations on what the proposed order permits the government to do.²⁴⁹ So before the government submits its official application, it has at least a general idea of what the FISA judge is prepared to approve. It is this practice that likely explains, at least in part, the government's overwhelming rate of success in FISA applications.²⁵⁰ A FISA judge can alert the government if a particular application is not going to pass muster, and the government has the opportunity to revise the application before making an official submission.

This process was particularly intense when it came to the bulk collection programs. Recall the numerous hearings the FISC held and the numerous government officials from which it received briefings.²⁵¹ These exchanges would have permitted the court and the government to determine together what minimization procedures should apply. They provided the court the opportunity to air its concerns and allowed the government to suggest the most efficient ways to mitigate those concerns. By the time the government submitted its bulk collection applications, the applications *themselves* proposed the vast majority of the minimization procedures that ended up in the court's orders. It is reasonable to think that the proposed procedures were the result of a bargain struck between the government and the court—the FISC would approve the government's bulk collection so long as the

248. SAVAGE, *supra* note 230, at 200.

249. Letter from Reggie B. Walton, Presiding Judge, FISA Court, to Honorable Patrick J. Leahy, Chairman, Senate Comm. on the Judiciary, at 5–7 (July 29, 2013), <https://www.leahy.senate.gov/imo/media/doc/Honorable%20Patrick%20J%20Leahy.pdf>.

250. Note that prior to 2007, the Justice Department knew the sitting schedule for the FISA judges, and at times used that information to submit controversial applications to judges inclined to agree with the government. SAVAGE, *supra* note 230, at 202.

251. *See supra* Section III.B.1.

government took measures to protect individual privacy interests.²⁵² So while the court was too weak to say no, the government's desire for approval did provide some negotiating leverage. And the court used that leverage to impose the rules it thought appropriate—rules that imported Fourth-Amendment-inspired protections.

Using this method of quasi-constitutional rulemaking has many advantages. If the Constitution does not apply, the court and the government are free to devise any mutually beneficial arrangement they can conceive. In negotiated-settlement territory, doctrine is no longer what matters. What matters is finding a way for each side to achieve its own goals. If the government is subject to limitations that the court believes to be sufficiently effective in protecting the interests it cares about, the ultimate authority for those limitations is essentially irrelevant. So, in devising with the government a set of minimization procedures to protect the privacy of U.S. persons, the FISC was able to further the constitutional principle of individual privacy while avoiding grounding the decision in constitutional interpretation.

Another advantage of such informal arrangements is that they avoid constitutional confrontations between the courts and the political branches. Regardless of the outcome of such a confrontation, it will undermine the legitimacy of both the courts and the political branch involved. If both the court and the government can achieve their goals by forging a mutually beneficial agreement instead, they turn a lose-lose situation into a win-win.

Relying on negotiated bargains rather than constitutional doctrine also provides the government and the court enormous flexibility in crafting their compromise.²⁵³ This flexibility might be a particularly valuable thing in areas of law subject to rapid and unpredictable changes, such as technological advancement of surveillance abilities. A judicial decision finding particular surveillance activities contrary to the Constitution would eliminate a potentially valuable tool. If the court is able to find a way to permit the government to use that tool without sacrificing constitutional values—in other words, through the

252. See *In re* Production of Tangible Things From [REDACTED], No. BR 08-13, Order, at 11 (FISA Ct. Mar. 2, 2009) (describing bulk collection minimization procedures as a “critical element” for securing the FISC’s approval).

253. See Monaghan, *supra* note 193, at 27 (citations omitted) (noting that constitutional rulings are more difficult to change and therefore permit less flexibility to future decision makers).

771 *Quasi-Constitutional Protections and Government Surveillance*

protection of quasi-constitutional rights rather than explicit constitutional rights—policy flexibility is preserved.

Finally, these mechanisms allow courts to identify some territory as constitutionally problematic. By articulating a result that avoids the need to define the exact scope of a constitutional right, a court can create a robustly defended right hung with a *proceed-with-caution* sign for policymakers. Quasi-constitutional rules can therefore protect constitutional values and provide policymaking guidance without having to commit to a particular constitutional interpretation.

Congress took advantage of that flexibility in 2015 when it enacted the USA FREEDOM Act (USAF). That legislation provided an explicit statutory basis for a modified version of the telephone metadata program.²⁵⁴ USAF codifies many of the ideas first introduced as minimization rules by the FISA Court, including the “reasonable, articulable suspicion” standard.²⁵⁵ The difference between USAF and the bulk telephony metadata collection program that preceded it, is that to query telephone data—now held by the telephone companies rather than the government—the statute requires the government show the FISC that the RAS standard has been met for each individual selector (specific selection term (SST), in the language of the statute) before conducting queries using that SST.²⁵⁶ In other words, the executive branch itself is no longer empowered to determine when a particular query is authorized. Had the FISC insisted that, as a constitutional matter, the government meet a probable cause standard before querying metadata databases, it would have taken that policymaking decision out of Congress’ hands. Of course those who reject the validity of any surveillance that does not require the government to show probable cause, provide particularity, and seek approval from a neutral decision maker may not see this flexibility as a boon. But in an area like counterterrorism, where both the threat and the available means of combatting it are constantly changing in unpredictable ways, the use of quasi-constitutional means of protecting individual rights might afford the government much-needed agility that the announcement of constitutional rules would eliminate.

254. USA FREEDOM Act of 2015, Pub. L. No 114-23, § 103, 129 Stat. 268, 272 (2015) (codified as amended at 50 U.S.C. §§ 1801–1885(c) (Westlaw through Pub. L. No. 114-219)) (“Prohibition on Bulk Collection of Tangible Things.”).

255. *Id.* § 101(a)(3)(C)(ii), 129 Stat. at 270.

256. *See id.* § 101(a)(3)(C)(i), 129 Stat. at 270.

CONCLUSION

As it turns out, the FISC's insistence on maintaining a role in surveillance oversight proved extremely meaningful. Throughout the course of the bulk collection programs' existence, the FISC's minimization procedures repeatedly led the government to discover (and to report to the FISC) issues of over-collection or other non-compliance. These discoveries in turn permitted the FISC to modify the minimization procedures to prevent such non-compliance in the future and to monitor the government's success in correcting non-compliant behavior.²⁵⁷ The FISC's participation thus prevented over-collection and misuse of information that otherwise would have been far more widespread and possibly gone undetected indefinitely.

This indicates that the court was at least partially successful in achieving its goals. It was able to impose quasi-constitutional rules, denying the intelligence community a surveillance blank check, while at the same time avoiding a constitutional confrontation with the executive branch—a confrontation it was likely to lose. It charted a middle path aimed at reinserting traditional Fourth Amendment principles of targeting and particularity through the use of minimization procedures. The minimization procedures that the FISC imposed on the bulk collection were, in a sense, the price of the court's approval. They represented a compromise that, while not entirely reinstating traditional Fourth Amendment protections, permitted the court to substitute rules aimed at protecting the same interests as does the Fourth Amendment, while simultaneously allowing the bulk collection of metadata. One view of this bargain is that it was actually a deal with the devil, and the FISA Court should not have approved bulk collection under any circumstances. Another is that in order to maintain its own relevance, the court turned to a familiar means of addressing threats to the constitutionality of surveillance—minimization procedures—to impose on the government quasi-constitutional limits, despite the position of weakness from which it was operating.

257. See generally *In re* [REDACTED], No. PR/TT [REDACTED], Memorandum Opinion, (FISA Ct. Nov. 30, 2011); *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 09-13, Order Regarding Further Compliance Incidents, at 2-4 (FISA Ct. Sept. 25, 2009).