Indiana Law Journal

Volume 91 | Issue 4 Article 4

Summer 2016

The Two Faces of the Foreign Intelligence Surveillance Court

Emily Berman
University of Houston Law Center, eberman@central.uh.edu

The Two Faces of the Foreign Intelligence Surveillance Court

EMILY BERMAN*

When former National Security Agency contractor Edward Snowden leaked a massive trove of information about secret intelligence-collection programs implemented under the Foreign Intelligence Surveillance Act in the summer of 2013, U.S. surveillance activities were thrust to the forefront of public debate. This debate included the question of whether and how to reform the Foreign Intelligence Surveillance Court ("FISA Court"), the statutorily created secret court that reviews government applications to conduct surveillance in the United States. This discussion, however, has underemphasized a critical feature of the way the FISA Court works. As this Article will show, since the terrorist attacks of September 11, 2001 ("9/11"), the FISA Court has been playing not only its traditional role of "gatekeeper," but also the additional—and entirely different—role of "rule maker." This is the first scholarly examination of this dichotomy and its implications for reform. Further, the Article is particularly timely in providing an assessment of the recently enacted USA FREEDOM Act of 2015, Congress's attempt to reform the court. I argue that, viewed through the lens of the court's dual roles, the scholarly and public conversation has fallen short in two important respects. First, it has failed to give the court sufficient credit for its laudable performance as gatekeeper, and second, it has ignored the implications that the gatekeeper/rule-maker dichotomy has for reform. As a result, I conclude that the USA FREEDOM Act is not only woefully inadequate to remedy the problems that it targets but also fails entirely to address additional problems with the FISA Court. In light of these conclusions, the USA FREEDOM Act represents a missed opportunity. In not fully appreciating or accounting for the unique challenges that the court's rule-making function poses, the Act does not go nearly far enough in bolstering the court's rulemaking competence. Moreover, the Act neglects (as has the public debate) a critical area for reform: ensuring sufficient flow of information from the executive branch to the FISA Court. I therefore explore the nature of this challenge and offer some additional reform ideas for consideration.

---

* Assistant Professor, University of Houston Law Center. Thanks go to Aaron Bruhl, Darren Bush, Geoff Corn, Lonny Hoffman, Aziz Huq, David Kwok, Peter Linzer, Jessica Mantel, Tom Oldham, Theodore Rave, Jessica Roberts, Steve Vladeck, Kellen Zale, and participants in the SEALS New Scholars Program.

INTRODUCTION

Former National Security Agency (NSA) contractor Edward Snowden's leak of a massive trove of information about formerly secret intelligence-collection programs in the summer of 2013 prompted a dramatic shift in public awareness of U.S. surveillance activities. Almost overnight, the American public learned of several aggressive intelligence-collection programs—including programs that collected significant amounts of information about innocent Americans—the most controversial of which were implemented under the auspices of the Foreign Intelligence Surveillance Act of 1978 (FISA).[1] These disclosures sparked vigorous debate about U.S. surveillance policy and generated significant momentum for statutory reform. Most reform discussion revolved around how to modify the government's highly controversial program of collecting and storing vast databases of domestic telephony metadata.[2] And when the surveillance debate culminated this past summer with the enactment of the USA FREEDOM Act of 2015,[3] Congress did indeed place limits on such activity.[4]

In addition to debate over what substantive surveillance authorities the government should possess, however, both the Snowden revelations and the ensuing conversation also shined a spotlight on an obscure institution: the Foreign Intelligence Surveillance Court ("FISA Court").[5] The FISA Court, statutorily created as part of FISA in 1978, reviews government applications for foreign intelligence surveillance orders—that is, confers approval to engage in surveillance. It was created to provide judicial supervision of the federal government's foreign intelligence–collection activities inside the United States. Information revealed in the wake of the Snowden leaks called into question the FISA Court's effectiveness in this role. One of the elements of the debate over surveillance reform thus became the question of whether and how to reform the FISA Court itself.

This Article argues that a critical—and underappreciated—element of this discussion is the fact that the FISA Court actually plays two very different roles. Its

---

1. Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended in scattered sections of the U.S.C.).

2. Metadata generally is defined as data that describes and gives information about other data. Communication metadata is information about the communication per se, including session identifying information (e.g., originating and terminating telephone number or e-mail address, communications device identifiers like IP addresses, etc.), routing information, time and duration of calls, and similar non-content information.

3. Pub. L. No. 114-23, 129 Stat. 268 (2015) (to be codified in scattered sections of the U.S.C.).

4. Whether preexisting law authorized the government's collection of phone data is a matter of vigorous debate, but the USA FREEDOM Act plainly limits bulk collection. *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23 sec.103, sec. 201, 129 Stat. 268, 272, 277 (to be codified at 50 U.S.C. §§ 1861, 1842).

5. For details on the creation, operation, and evolution of the FISA Court, see *infra* Part I.A.

original and traditional role is that of "gatekeeper." Since 9/11, however, the court has been forced to play an additional, entirely distinct function—that of "rule maker."[6]

When the FISA Court operates as a gatekeeper, it acts as a watchdog. As gatekeeper, the court evaluates whether government surveillance requests comply with legal requirements, much the way a magistrate judge reviews applications for search or arrest warrants.[7] In other words, the court first screens government requests to engage in surveillance of a particular target, applying clearly established law to a specific set of circumstances and approving only those collection activities that comply with applicable requirements and restrictions. If the court determines that a government application should be approved, it issues an appropriate order. Matters requiring it to play this gatekeeper function are what the FISA Court was created to handle and still form the vast bulk of its docket.

Since 9/11, however, the court has also been asked to play a new role, what I call its rule-maker role. This role is triggered when the court is asked whether bulk-collection programs comply with both FISA and the Constitution. The defining characteristic of "bulk collection" programs—in contrast to "targeted collection" programs—is that a significant portion of the collected data is not associated with specific targets or subjects of interest in a particular investigation. When approving government surveillance programs that do not involve case-by-case assessments of each proposed target, FISA judges do not simply evaluate whether a particular surveillance request meets the necessary requirements—whether, for example, the government has established probable cause. Rather, they must determine whether the rules under which the government has proposed to operate while collecting information in bulk satisfy existing law. This rule-maker responsibility represents an enormous alteration of the FISA Court's docket, forcing it to play a role for which it was not designed and is not well suited.

A handful of others have recognized that the court is doing something new of late, but this is the first scholarly article to examine closely the dichotomy between gatekeeper and rule maker and to explore its implications for reform. I argue that discussion surrounding the FISA Court has failed to appreciate the significance of this dichotomy. As a result, the public conversation has fallen short in two important respects. First, it has failed to give the court sufficient credit for its laudable performance as gatekeeper and the extent of oversight in which it has engaged in that capacity. Indeed, when in possession of all the relevant information, FISA judges-as-gatekeepers have aggressively employed the equitable powers of the courts to serve as a meaningful check on the government's bulk surveillance activities.[8] Second, while critiques of the FISA Court in its rule-maker role are fully justified—the court's rulemaking has displayed incomplete analysis, relied upon

---

6. If the term "rule maker" invokes thoughts of administrative law, it is no accident. What I call the FISA Court's rule-making activities resemble nothing so much as agency rule making. The resemblance of the FISA Court to an administrative agency, and the implications of that resemblance, is an area for future research.

7. *See, e.g.*, FED. R. CRIM. PRO. 41(d) (authorizing a warrant "if there is probable cause to search for and seize a person or property or to install and use a tracking device").

8. *See infra* Part II.A.

unconvincing reasoning, and failed to consider important counterarguments[9]—they have ignored the implications that the gatekeeper/rule-maker dichotomy has for reform.

These conclusions permit me to turn the lens of the court's dual roles on the recently enacted USA FREEDOM Act to assess the sufficiency of its reforms to the court.[10] Given the court's failure as rule maker, the USA FREEDOM Act represents nothing so much as a missed opportunity. In not fully appreciating or accounting for the unique challenges that the court's rulemaking function poses, the USA FREEDOM Act does not go nearly far enough in bolstering the court's rulemaking competence. It does include measures that gesture in the right direction—increasing the adversarial nature of the FISA Court's proceedings, augmenting the availability of appellate review of FISA judges' decisions, adding transparency to the court's operations, and increasing FISA judges' access to technical expertise—but these will prove woefully inadequate. Moreover, the Act neglects (as has the public debate) a critical area for reform that will play to the FISA Court's strength as gatekeeper: ensuring sufficient flow of information from the executive branch to the FISA Court. I therefore explore the nature of this challenge and offer some additional reform ideas for consideration.

Part I of this Article will lay out first the relevant aspects of the FISA Court's operations and then the critiques of those operations. Part II will look closely at the FISA Court's performance as gatekeeper and as rule maker in the approval and oversight of bulk-collection programs and argue that the FISA Court has performed its gatekeeper function well while failing in its rule-maker function. Part III will consider the implications of the FISA Court's strengths and weaknesses, as set out in Part II, for reform as well as critique the USA FREEDOM Act's reforms to the court, pointing out areas in which the Act falls short, as well as areas that it overlooked altogether.

I. THE FISA COURT DEBATE

The FISA Court has never been entirely uncontroversial, but with the trove of new information about the court and its operations revealed by Edward Snowden—and by the government in response to the Snowden leaks—controversy over the court entered the public debate like never before. Part I.A will discuss the FISA Court's operations, elaborating further on the court's dual role as gatekeeper and rule maker; Part I.B will then catalog the primary critiques leveled at those operations.

A. The Foreign Intelligence Surveillance Court

The FISA Court was created in 1978 by FISA as part of a comprehensive regime to impose limits on and oversight of the domestic use of surveillance for the collection of foreign intelligence.[11] FISA itself was in part a response to revelations

9. *See infra* Part II.B.

10. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (to be codified in scattered sections of 50 U.S.C.).

11. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended in scattered sections of the U.S.C.).

in the early 1970s that the U.S. intelligence community had for decades engaged in unethical and illegal intelligence collection because intelligence agencies lacked "appropriate restraints, controls, and prohibitions."[12] Recognizing that "warrantless electronic surveillance in the name of national security ha[d] been seriously abused," Congress and the executive branch agreed not only to subject those activities to substantive limits but also to employ Article III judges in ensuring that those limits were respected.[13] As Senator Birch Bayh stated during the original Senate debate on FISA, the Act was intended to "bring an end to the practice of electronic surveillance by the executive branch without a court order in the United States."[14] The result was the FISA Court.

The court itself currently comprises eleven federal judges, chosen by the Chief Justice of the U.S. Supreme Court from among sitting U.S. district court judges, to serve staggered seven-year terms.[15] The membership of the FISA Court at any given time is public information, but the vast majority of its work—its proceedings, orders, and opinions—has traditionally remained secret.[16] FISA also created a FISA Court of Review, made up of three federal district or appeals court judges appointed by the Chief Justice, to hear appeals from decisions of judges on the FISA Court.[17]

While the contemporary FISA Court plays two roles, it was originally designed to play just one—gatekeeper. As law and technology have changed over time, however, it has taken on a second role—rule maker. The balance of this Part will specify what each of those roles encompasses and the FISA Court procedures through which they are exercised.

---

12. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, INTELLIGENCE ACTIVITIES AND RIGHTS OF AMERICANS: BOOK II, S. REP. NO. 94-755, at 171 (1976) [hereinafter CHURCH COMM. REPORT], *available at* http://www.intelligence.senate.gov/sites/default/files/94755_II.pdf [https://perma.cc/3KAY-GZ9N].

13. SENATE COMM. ON THE JUDICIARY, FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, S. REP. NO. 95-604, pt. 1, at 7 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908; *see also* CHURCH COMM. REPORT, *supra* note 12, at 292 (identifying excessive concentration of power in the executive as one source of rights violations).

14. 124 CONG. REC. 10889–90 (1978) (statement of Sen. Birch Bayh); *see also Foreign Intelligence Surveillance Act: Hearings Before the Subcomm. on Courts, Civil Liberties, & the Admin. of Justice of the H. Comm. on the Judiciary*, 94th Cong. 28–29 (1976) (statement of Hon. Philip Lacovara, former Deputy Solicitor General) (noting that FISA required judicial involvement because "the courts, from the earliest time, have been regarded as the bulwarks of liberty against executive excesses," and because executive branch officials exercise greater self-restraint when forced "to justify [decisions] to someone else").

15. 50 U.S.C.A. § 1803(a), (d) (West 2015). The FISA Court originally comprised seven judges; that number was expanded to eleven in the USA PATRIOT Act of 2001. Pub. L. No. 107-56, sec. 208, § 103(a), 115 Stat. 272, 283 (codified as amended at 50 U.S.C. § 1803(a)).

16. *See Current Membership—Foreign Intelligence Surveillance Court*, U.S. FOREIGN INTELLIGENCE SURVEILLANCE CT., http://www.fisc.uscourts.gov/current-membership [https://perma.cc/B3D5-8CRX]. The USA FREEDOM Act aims to make more opinions and orders public, but FISA Court proceedings will remain secret. USA FREEDOM Act of 2015, Pub. L. No. 114-23, sec. 402, § 602, 129 Stat. 268, 281–82 (to be codified at 50 U.S.C. § 1872).

17. 50 U.S.C.A. § 1803(b).

1. The FISA Court's Original Role: Gatekeeper

Prior to the passage of the USA PATRIOT Act in 2001[18]—which amended portions of FISA—and the FISA Amendments Act of 2008,[19] the nature of FISA's statutory requirements for intelligence collection dictated a narrow scope for the court's operations. Its role was limited to evaluating ex parte applications for intelligence collection directed at specific, individual targets.[20] Indeed, at the time of FISA's passage, the fact that FISA judges would be "applying the law to the facts of a particular case" alleviated concerns that the ex parte nature of the court's proceedings might violate Article III's case or controversy requirement.[21] This is what I call the court's gatekeeper function.

As gatekeepers, FISA judges' evaluations of applications for intelligence-collection orders are analogous to that of magistrate judges considering applications for search warrants or wiretapping authority in the criminal context.[22] The FISA judge must make an independent determination of whether the government has met the standard necessary. Before approving electronic surveillance of an individual's communications inside the United States, for example, the FISA judge must determine that there is probable cause to believe that the target of the surveillance is either a foreign power or its agent, that the places at which the surveillance is targeted are used by the foreign power or its agent,[23] and that the government's proposed minimization procedures—procedures designed to limit the acquisition, retention, and dissemination of nonpublicly available information about unconsenting United States persons—satisfy the statutory standard.[24] Only after

---

18. Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S.C.).

19. Pub. L. No. 110-261, 122 Stat. 2436 (2008) (codified as amended in scattered sections of the U.S.C.).

20. The applications, which require the Attorney General's approval, are generated in the National Security Division—a division of the Department of Justice—on behalf of, and in coordination with, the agency requesting surveillance authority. Letter from Hon. Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to Hon. Patrick J. Leahy, Chairman, Senate Committee on the Judiciary, at 2 n.3 (July 29, 2013). The NSA implements approved requests for signals-intelligence collection—intelligence derived from electronic signals and systems, such as communications systems, radars, and weapons systems. NSA, THE NATIONAL SECURITY AGENCY: MISSIONS, AUTHORITIES, OVERSIGHT AND PARTNERSHIPS 2 (2013), *available at* https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf [https://perma.cc/7LX2-4FW7].

21. ELIZABETH GOITEIN & FAIZA PATEL, BRENNAN CTR. FOR JUSTICE, WHAT WENT WRONG WITH THE FISA COURT 7 (2015).

22. *See supra* note 7 and accompanying text (discussing search and seizure warrants); *see also* 18 U.S.C. §§ 2510–2522 (2012) (setting out rules governing electronic surveillance in the domestic criminal context).

23. 50 U.S.C.A. § 1805(a)(2) (West 2015).

24. *Id.* § 1805(a)(3). Minimization procedures are defined as:

> (1) specific procedures . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons . . . ;

determining that the government has successfully established each of these elements may the court issue an order approving the surveillance.

The FISA Court's jurisdiction originally was limited to oversight of electronic surveillance, but over time it has expanded to cover physical searches, the use of pen registers/trap-and-trace devices (pen/traps),[25] and the production of tangible things as well.[26] Each of these surveillance methods has its own requirements that the government must meet.[27] Should the judge require additional information to make the required determinations, she may require the applicant to furnish it.[28]

Evaluation of these types of applications demands a narrow inquiry into whether the government has adequately satisfied FISA's defined requirements. In other words, the question is whether the government has included all of the required elements in its application and successfully established the necessary standard—for example, probable cause, in the case of electronic surveillance. If each requirement is met, the FISA judge may issue an order permitting the requested activity.[29]

So as originally conceived, a FISA judge's job is to evaluate government requests for authority to collect intelligence from a specific person, and from a specific place or communications device, and to ensure that the government's implementation of that authority complies with constitutional, statutory, and judicially ordered limits.[30] In performing this work, FISA judges are primarily assisted not by the usual cadre of clerks culled from recent law school graduates, but instead by full-time legal counsel who are employees of the Justice Department.

> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information . . . shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
> (3) . . . procedures that allow for the retention and dissemination of information that is evidence of a crime . . . ; and
> (4) . . . procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours . . . .

50 U.S.C.A. § 1801(h) (West 2015).

25. Pen registers record outgoing communications metadata; trap-and-trace devices record the incoming information. *See infra* note 38.

26. 50 U.S.C.A. § 1861 (West 2015).

27. To acquire business records, the government must establish that there are "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation." *Id.* § 1861(b)(2)(A). For a pen/trap order, the government must show that the information "likely to be obtained is foreign intelligence information . . . or is relevant to an ongoing investigation." 50 U.S.C.A. § 1842(c)(2) (West 2015).

28. 50 U.S.C. § 1804(c) (2012).

29. 50 U.S.C.A. § 1805(a) (West 2015).

30. For a more detailed discussion of courts' ex parte review of government applications, see Orin S. Kerr, *A Rule of Lenity for National Security Surveillance Law*, 100 VA. L. REV. 1513, 1516–18 (2014).

2. The FISA Court's New Role: Rule Maker

After 9/11, the FISA Court's role expanded beyond assessing the lawfulness of requests for intelligence-collection orders directed at a particular target. Instead, it has also been asked to approve a very different kind of surveillance—bulk surveillance. Bulk surveillance refers to broad collections programs that do not require judicial approval on a case-by-case basis. Rather than determining the lawfulness of a particular instance of surveillance, the court pronounces whether an entire surveillance program complies with the statute and the Constitution. Issuing opinions regarding the validity of programmatic or bulk-collection programs—what I refer to as the FISA Court's rule making—represents a sea change in the court's responsibilities.

The FISA Court has authorized at least three bulk-collection programs since 9/11, some more controversial than others. The most controversial is the bulk collection of all domestic telephony metadata pursuant to section 215 of the USA PATRIOT Act, also known as the FISA business records provision.[31] Section 215 permits the government to collect "any tangible thing[]" that is "relevant" to an ongoing investigation.[32] Under this provision, the government can noncontroversially engage in targeted collection—to access a suspected foreign agent's banking information or credit card records, for example. Under the bulk-collection program, however—referred to variously as the section 215 program, the telephony metadata program, or the telephone bulk-collection program—the NSA did not seek out specific items related to a specific target. Instead, it collected telecommunications companies' entire databases of records for all domestic phone calls. The information collected included (at a minimum) the telephone numbers dialed and the dates, times, and duration of calls.[33] The NSA could then "query," or search, this database using terms, known as "seed identifiers" (usually phone numbers), in an effort to identify as-yet-unknown terrorist suspects.[34] After the section 215 program became public, President Obama curtailed its scope slightly;[35] it was then permitted to expire just prior to the passage of the USA

---

31. 50 U.S.C.A. § 1861(a)(1) (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, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution").

32. *Id.*

33. ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 3 (2013) [hereinafter ADMINISTRATION SECTION 215 WHITE PAPER].

34. One method through which this is attempted is known as "contact chaining," or analysis of the connections between seed identifiers and others. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 8–9 (2014) [hereinafter PCLOB SECTION 215 REPORT].

35. Remarks on United States Signals Intelligence and Electronic Surveillance Programs, 2014 DAILY COMP. PRES. DOC. 6–7 (Jan. 17, 2014) [hereinafter Remarks on United States Signals Intelligence].

FREEDOM Act, which enacted several modifications to section 215 itself.[36] The second bulk-collection program under the FISA Court's oversight (voluntarily discontinued by the executive branch in 2011)[37] allowed bulk collection of Internet metadata through the use of the FISA pen/trap provision.[38] The third bulk-collection program, which is currently ongoing, is known as the section 702 program—named for a statutory provision of the FISA Amendments Act—which authorizes the bulk collection of the contents of communications when the target is reasonably believed to be outside the United States, even if the target's interlocutor is in the United States.[39] Under these bulk-collection programs, the court need not approve each surveillance target; indeed, it likely does not know what the specific targets of surveillance will be.

I am not the first to recognize the novelty of this role. Indeed some have argued that adding this function to a court designed to operate only as a mechanism to approve individualized surveillance is at best unwise and at worst unconstitutional.[40] But even assuming that assigning the FISA Court a rule making role is neither unwise nor unconstitutional, it is crucial to recognize just how different it is. Both former FISA Court Judge James Robertson and an independent commission established by President Obama in the wake of the Snowden revelations—the President's Review Group on Intelligence and Communications Technologies (President's Review Group)—noted the change.[41] During his time on the court, Robertson explained,

---

36. 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?_r=0 [https://perma.cc/CXZ4-8HH6]; 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 [https://perma.cc/JY2D-8XQ7].

37. *See* 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 [https://perma.cc/432R-9PGG].

38. Pen registers record outgoing communication information, such as the numbers called from a particular phone; trap-and-trace devices record information about incoming communications. *See generally* 50 U.S.C.A. § 1842 (West 2015) (permitting "the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution").

39. Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2438–48 (2008) (codified as amended in scattered sections of the U.S.C.).

40. *E.g.*, GOITEIN & PATEL, *supra* note 21, at 29–32.

41. *Id.* at 30. President Obama established the President's Review Group, shortly after the Snowden leak, to determine how "the United States can employ its technical collection capabilities in a manner that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties." Press Release, Statement by the Press Secretary on the Review Group on Intelligence and Communications Technology (Aug. 27, 2013), *available at* https://www.whitehouse.gov/the-press-office/2013/08/27/statement-press-secretary-review-group-intelligence-and-communications-t [https://perma.cc/3ARC-YJT5].

judges had no need to issue opinions. "You approved a warrant application or you didn't, period."[42] In other words, the job was limited to gatekeeping. But the evolution of both technology and the law has "introduced a new role" for the FISA Court, turning it into "something like an administrative agency which makes and approves rules for others to follow."[43]

Congress explicitly expanded the FISA Court's role in the FISA Amendments Act of 2008 (FAA), which authorizes electronic surveillance in the absence of the type of specific inquiry that had formed the content of a FISA judge's work for the court's first thirty years.[44] Under the FAA, so long as the target is "reasonably believed to be located outside the United States" and is not a U.S. person, electronic surveillance is permissible.[45] But under the FAA, the FISA judge is not asked to determine whether the government has established probable cause that the proposed target is "reasonably believed to be located outside the United States." That is to say, the judge never determines whether an individual person, or an individual facility, meets specific requirements. Instead, the statute requires the judge to review the government's rules for targeting and decide whether those rules, in the abstract, are sufficiently likely to yield permissible targets.[46] So the question for the FISA judge becomes whether the government's targeting procedures are designed in such a way that, when used by the executive branch to select targets, those selected targets are "reasonably believed to be located outside the United States." Similarly, the judge must assess whether the government's proposed rules governing minimization, in the abstract, provide sufficient protection to U.S. person information.[47] In other words, the court must assess the statutory and constitutional sufficiency of the entirety of the program, rather than assessing whether any given proposed target falls within FISA's purview. In reviewing whether the government's proposed targeting and minimization procedures were sufficiently likely to yield permissible surveillance activities, the court is not adjudicating the validity of an instance of government surveillance; it is making and approving rules that government agencies are bound to follow. In other words, the FAA forced the FISA Court to become a rule maker.

---

42. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., WORKSHOP REGARDING SURVEILLANCE PROGRAMS OPERATED PURSUANT TO SECTION 215 OF THE USA PATRIOT ACT & SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 90 (2013) [hereinafter PCLOB WORKSHOP] (statement of Hon. James Robertson). Robertson sat on the FISA Court from 2002–2005. Stephen Braun, *Former FISA Judge Says Secret Court Is Flawed*, YAHOO! NEWS (July 9, 2013), *available at* https://www.yahoo.com/news/former-fisa-judge-says-secret-court-flawed-201422173.html?ref=gs [https://perma.cc/U4DV-7STH].

43. *Id.* at 36 (statement of Hon. James Robertson); *see also* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 203 (2013) [hereinafter PRESIDENT'S REVIEW GRP. REPORT]. The President's Review Group's final report made forty-six recommendations, including several specifically related to the FISA Court. *Id.* at 200–08.

44. PCLOB WORKSHOP, *supra* note 42, at 36 (statement of Hon. James Robertson) ("Congress passed the FISA Amendments Act of 2008 and introduced a new role for the [FISA Court], which was to approve surveillance programs.").

45. 50 U.S.C.A. § 1881a(b)(3), (g)(2) (West 2015).

46. *Id.* § 1881a(i)(2).

47. *Id.*

Questions regarding bulk collection posed by the section 215 metadata program arose out of both legal and technological changes.[48] Prior to 9/11, to secure an order under section 215, the government had to provide "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[49] In October 2001, the USA PATRIOT Act amended the provision so that an order requires merely "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation."[50] This new version of section 215 seems to require individualized surveillance approval, albeit according to a lower standard. Unbeknownst to the public, however, the government advocated for a novel legal interpretation of section 215 that would allow the NSA to take advantage of technological capacities to collect and retain information about a vast number of individuals in order to search for information relevant to an investigation later. Thus, when faced with the initial government application seeking telecommunications companies' database of records for all domestic phone calls, the FISA judge on duty that week had to assess whether section 215 could be interpreted to permit such collection.[51] In approving the program, the FISA Court ruled that the collection of an entire database was permissible under section 215, so long as the government queried that information using only search terms for which there was "reasonable articulable suspicion" that the term was related to international terrorism.[52] Rather than making a determination itself with respect to whether each search term satisfied the "reasonable articulable suspicion" standard, however, the court ceded to the government the authority to make that determination for itself. In other words, it set out the rule by which the government was authorized to access the bulk data and left it to the government to follow that rule.

A similar question had previously arisen in the context of the bulk collection of Internet communications metadata under FISA's pen/trap provision. Recognizing that it was asking the court to do something unusual, the government submitted lengthy briefs setting out its desired interpretation of the pen/trap provision as part of its initial application for approval.[53] And the assigned FISA judge issued a lengthy opinion explaining her reasoning in approving the practice.[54] So both the government and the FISA Court itself have recognized that the post-9/11 surveillance statutes, or the government's interpretation of those statutes, have resulted in a massive modification of the FISA Court's responsibilities. Despite these substantive modifications to the court's responsibilities, however, there have been only minor

---

48. Kerr, *supra* note 30, at 1522 (stating that because surveillance agencies are "at the leading edge" of quickly evolving technology, ambiguities in surveillance statutes are likely to develop).

49. 50 U.S.C. § 1862(b)(2)(B) (2000).

50. 50 U.S.C. § 1861(b)(2)(A) (2012).

51. Kerr, *supra* note 30, at 1528–30.

52. *See infra* text accompanying notes 101–03.

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

54. Opinion and Order, *In re* [REDACTED], No. PR/TT [REDACTED] (FISA Ct. July 14, 2004) [hereinafter Judge Kollar-Kotelly's Pen/Trap Opinion].

changes to the court's procedures. As a result, a court designed to accomplish one purpose is now being asked to add another, but without any consideration of whether the court's design can accommodate that new purpose. As I discuss in Part II.B, it turns out that the FISA Court's original design is not well suited to the new task of rule making.

B. Critiques of the FISA Court

Critiques of the FISA Court have come from a spectrum of sources—academic commentators, privacy and civil liberties advocates, government review boards, and even former members of the court itself. Each of them has consistently focused on a similar set of concerns related to the court's operation—the most frequent points focus on the court's nonadversarial nature and the resulting scarcity of appeals as well as its lack of transparency. Other concerns surround the way the FISA judges are selected and whether the court has the information it needs.

1. The FISA Court's Proceedings Are Not Adversarial

Prior to 2007, FISA contemplated no adversarial proceedings at all. But Congress seems to have recognized that it was changing the FISA Court's role when it included in the FISA Amendments Act a provision under which recipients of FISA Court orders requiring them to provide information about their subscribers could challenge those orders in an adversarial proceeding.[55] Because the court would no longer provide a judicial check on the executive branch's targeting decisions, Congress looked for another means to challenge executive branch actions. This mechanism has proved toothless, however, because it allows recipients of orders (communications service providers) to challenge them, but not targets of orders (those being surveilled). Service providers rarely will have the incentive necessary to prompt them to challenge government orders. To date, just one service provider—Yahoo—has availed itself of this opportunity pursuant to the Protect America Act of 2007, the precursor to the FISA Amendments Act, and none has done so under the FISA Amendments Act itself. Congress did not include even this watered-down adversarial process in the FISA Court's other rule-making contexts. In addition to this one adversarial matter, there have been a handful of instances in which a FISA judge has entertained various motions from nongovernmental entities or agreed to permit some to participate as amici.[56] The frequency with which the FISA Court has overseen adversarial proceedings is thus vanishingly small.

The FISA Court has been strongly criticized for its dearth of adversarial proceedings. Adversarial proceedings are the norm in the United States' judicial

---

55. 50 U.S.C.A. § 1881a(h)(4)(A) (West 2015) (providing that communication service providers who receive an order under section 702 "may file a petition to modify or set aside such directive" with the FISA Court). The provision was initially enacted in the Protect America Act of 2007 (PAA). Pub. L. No. 110-55, sec. 2, § 105B, 121 Stat. 552, 552 (2007) (allowing the government to acquire "foreign intelligence information concerning persons reasonably believed to be outside the United States") (codified at 50 U.S.C. § 1805b) (repealed). When the FISA Amendments Act took the PAA's place, it retained this provision.

56. Letter from Hon. Reggie B. Walton, *supra* note 20, at 9–10 (listing instances).

system[57] based on the idea that "the adversary system is an engine of truth [that assumes] that judges are in a better position to find the right answer . . . when they hear competing views."[58] FISA judges, by contrast, are not provided with counterarguments or critiques of the government's position. There is no institutional mechanism for pointing to flaws or weaknesses in the government's legal interpretations. According to an in-depth study of the section 215 program by the Privacy and Civil Liberties Oversight Board (PCLOB), an independent government agency created to examine the effects of counterterrorism policy on civil liberties,[59] "there is a growing consensus that the *ex parte* approach is not the right model" for at least some subset of applications for collection of "the communications of many people who have no apparent connection to terrorism."[60] These critiques are not aimed solely at FISA Court outcomes. Even assuming no outcomes changed, opinions from judges with the benefit of hearing arguments on all sides would be more thorough, thoughtful, and fully developed.[61] Moreover, as the result of effective procedures, the opinions would command more legitimacy.

Another concern regarding the lack of adversaries in the FISA Court's operations is the dearth of appeals of pro-government decisions.[62] Prior to the passage of the USA FREEDOM Act, which attempts to add some adversarial process to the FISA Court's operations, an appellate panel would almost never review FISA Court decisions unless the initial decision went against the government—a rarity.[63] The government has always had the power to appeal a denial of an application to the FISA Court of Review, and, in the event that the FISA Court of Review rules against the government (an event that, as far as the public knows, has never come to pass),

---

57. Kerr, *supra* note 30, at 1516 (citing Abram Chayes, *The Role of the Judge in Public Law Litigation*, 89 HARV. L. REV. 1281, 1285–86 (1976)).

58. PRESIDENT'S REVIEW GRP. REPORT, *supra* note 43, at 203; *see also* Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden*, 66 HASTINGS L.J. 1, 51–57 (2014) (arguing that an adversarial process would improve the FISA Court's reasoning).

59. The PCLOB is an independent executive branch agency established by the Implementing Recommendations of the 9/11 Commission Act of 2007. Pub. L. No. 110-53, sec. 801, 121 Stat. 266, 352 (2007) (codified as amended in scattered sections of the U.S.C.). The board has five members, who are appointed by the President and confirmed by the Senate. The board's enabling statute vests it with the authority to (1) review executive branch counterterrorism actions, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties, and (2) ensure that liberty concerns are appropriately considered in the development and implementation of counterterrorism laws, regulations, and policies. 42 U.S.C. § 2000ee (2012).

60. PCLOB SECTION 215 REPORT, *supra* note 34, at 183–84 (italics in original).

61. James G. Carr, *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 [https://perma.cc/9AKS-SZ8C].

62. *Id.*

63. For the USA FREEDOM Act's modifications in this area, see *infra* Part III.B. In the court's rare adversarial proceedings, the nongovernmental party may appeal adverse decisions to the FISA Court of Review and petition the Supreme Court for certiorari. 50 U.S.C. § 1881a(h)(6) (2012).

to petition the Supreme Court for a writ of certiorari.[64] There is no adverse party able to lodge an appeal when an order is granted. And except in the rare context of a service provider's challenge to an order under the FISA Amendments Act or the participation of an amicus, at no step in the process does the reviewing court hear from a party other than the government.

2. The FISA Court Lacks Transparency

The second common critique of the FISA Court has been its lack of transparency—another issue that the USA FREEDOM Act takes on.[65] Proponents of reform have argued that, like adversarial proceedings, transparency of judicial action is the norm and that exposing judicial proceedings to public scrutiny draws attention to flawed or unpersuasive rulings as well as potentially undesirable developments in the law.[66] Without transparency, the check on judicial action that comes from issuing a public, reasoned decision is absent. Moreover, when a judge's work will not be subject to public scrutiny and critique, it becomes easier for the judge to engage in incomplete, unconvincing, or otherwise flawed analysis.[67] Finally, citizens are more likely to trust in their government's good faith when a full account of its activities is available.

Historically, the FISA Court has lacked the benefits of transparency on several levels, only some of which are affected by the USA FREEDOM Act. In the United States, judicial proceedings are, as a rule, open to the public.[68] The FISA Court's rules, by contrast, explicitly provide that hearings "must be *ex parte* and conducted within the Court's secure facility," which is accessible only by individuals with the

---

64. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 103(b), 92 Stat. 1783, 1788 (codified at 50 U.S.C. § 1803).

65. *See infra* Part III.

66. *See, e.g.*, *The Administration's Use of FISA Authorities, Hearing Before the H. Comm. on the Judiciary*, 113th Cong. (2013) (statement of Jameel Jaffer, Deputy Legal Director, ACLU); PRESIDENT'S REVIEW GRP. REPORT, *supra* note 43, at 205–07; Alan Butler, *Standing Up to* Clapper*: How To Increase Transparency and Oversight of FISA Surveillance*, 48 NEW ENG. L. REV. 55, 86–88 (2013).

67. *See, e.g.*, Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609, 1640 (2012) (noting, in the context of criminal warrants, "police officers, cognizant of the fact that their warrant applications will be scrutinized carefully, will not bother filing weak applications"); Ashley S. Deeks, *The Observer Effect: National Security Litigation, Executive Policy Changes, and Judicial Deference*, 82 FORDHAM L. REV. 827, 833–56 (2013) (defining and providing examples of how interbranch interactions affect national security law and policy making); George L. Priest & Benjamin Klein, *The Selection of Disputes for Litigation*, 13 J. LEGAL STUD. 1, 4–6 (1984) (positing that, inter alia, litigants who do not expect to prevail at trial are more likely to avoid trial by settling).

68. *E.g.*, Richmond Newspaper, Inc. v. Virginia, 448 U.S. 555, 580 (1980) (holding that "the right to attend criminal trials is implicit in the guarantees of the First Amendment" (footnote omitted)); Neb. Press Ass'n v. Stuart, 427 U.S. 539, 570 (1976) (holding that prior restraints on media coverage of criminal trial are unconstitutional); Vincent Blasi, *The Checking Value in First Amendment Theory*, 1977 AM. B. FOUND. RES. J. 521.

appropriate security clearance.[69] Thus, all but a handful of proceedings are seen only by a limited number of government officials.

Perhaps more importantly, prior to the passage of the USA FREEDOM Act, FISA Court opinions also lacked transparency and were rarely released beyond the relevant congressional oversight committees. Indeed, prior to the Snowden revelations, none of the documents setting out arguments for the lawfulness of the government's bulk-collection programs were public. Since neither the FISA Court's orders nor its opinions are available, the American people know neither how the court is interpreting the law[70] nor what programs the government has implemented under its FISA authorities.[71]

3. The FISA Court Lacks Diversity

A third target of criticism is the method through which FISA judges are chosen, an area left untouched by the USA FREEDOM Act. FISA clearly anticipated that a relatively diverse set of judges would serve on the court at any one time. The eleven judges on the court must be selected from at least seven different judicial circuits[72] and must serve staggered terms,[73] so that the judges will have differing levels of FISA experience. In addition, a judge may sit on the FISA Court for only one term,[74] a rule that ensures that its ranks will be constantly refreshed from a broad pool of federal judges. Moreover, the constant turnover engendered by the seven-year terms ensures that as the Chief Justiceship changes hands, each new Chief Justice will have the opportunity to appoint his own selections to the FISA Court.

Despite these various rules, critics highlight the FISA Court's lack of diversity. Of the judges who currently serve, only one is a Democratic appointee to the bench.[75] In fact, as of 2014, only three of the twenty judges appointed to the FISA Court and the FISA Court of Review over the past decade have been Democratic appointees to the bench.[76] The President's Review Group argues that lack of party diversity can have predictable substantive effects. Republican- and Democratic-appointed judges often have divergent views on issues that the court often faces, such as "privacy, civil liberties, and claims of national security."[77] Thus, the President's Review Group's report asserts, there is a "legitimate reason for concern if, as is now the case, the

---

69. FISA CT. R. 17(b) (italics in original).

70. *The Administration's Use of FISA Authorities*, *supra* note 67, at 84–85 (statement of Jameel Jaffer, Deputy Legal Director, ACLU); Butler, *supra* note 67, at 86–88.

71. Butler, *supra* note 67, at 83–86; *see also* AM. BAR ASS'N., REPORT TO THE HOUSE OF DELEGATES (2002) (calling for "an annual statistical report on FISA investigations, comparable to the reports prepared for the Administrative Office of the United States Courts . . . regarding the use of Federal wiretap authority").

72. 50 U.S.C.A. § 1803(a)(1) (West 2015).

73. *Id.* § 1803(d).

74. *Id.*

75. Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 825 (2014); *Current Membership—Foreign Intelligence Surveillance Court*, *supra* note 16.

76. Donohue, *supra* note 76, at 825.

77. PRESIDENT'S REVIEW GRP. REPORT, *supra* note 43, at 207–08.

judges on the [FISA Court] turn out to come disproportionately from either Republican or Democratic appointees."[78] FISA judges are also likely to come from a background in prosecution or law enforcement—only one FISA judge has had significant experience as a public defender.[79] Moreover, given the young age at which most Chief Justices are selected and the concomitant length of their tenure on the Supreme Court, one person is granted the power to select all members of this important court for decades at a time.[80]

Proponents of the argument that the FISA Court is merely a rubber stamp for the government often blame the makeup of the court for this phenomenon. According to this argument, the court does not engage in meaningful gatekeeping when reviewing government applications, but instead simply approves them, providing the appearance of oversight without its substance. The court's rate of approval, which is over ninety-nine percent, is frequently provided as evidence of the court's status as a paper tiger.[81]

4. The FISA Court Judges Lack Necessary Information

One criticism of the FISA Court that has received insufficient attention to date is its potential for information deficits. The court potentially suffers from a dearth of two types of information—technical expertise regarding the government's surveillance capabilities and activities, and information regarding the ways in which the government is actually implementing its surveillance authority.

The surveillance programs that the court oversees employ complex and quickly evolving technological tools. The mechanics of these tools are not only highly technical, but also integral to mechanisms put in place to prevent misuse of surveillance powers or the resulting information.[82] Observers have pointed out that, to the extent these internal controls are based on an understanding of the structure of

---

78. *Id.* at 208.

79. Russell Wheeler, *The Changing Composition of the Foreign Intelligence Surveillance Court and What if Anything To Do About It*, LAWFARE RES. PAPER SERIES 1, 8 (2014).

80. Since 1953, the United States has had just four Chief Justices—Earl Warren (1953–1969), Warren E. Burger (1969–1986), William Rehnquist (1986–2005), and John Roberts (2005–present). *See Members of the Supreme Court of the United States*, SUPREME CT. OF THE U.S., http://www.supremecourt.gov/about/members_text.aspx [https://perma.cc/2U83-TZ9X] (listing all Chief and Associate Justices as well as their dates of service).

81. Over its first two and a half decades, the FISA Court approved nearly every single application without modification. 1 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS 469 (2d ed. 2012). Between 1979 and 2003, it denied only three out of 16,450 applications. LAURA K. DONOHUE, THE COST OF COUNTERTERRORISM: POWER, POLITICS, AND LIBERTY 232 (2008). And with respect to applications for section 215 orders specifically, "[i]t appears that [the FISA Court] has *never* denied [one.] That is, of 751 applications since 2005, all 751 have been granted." Donohue, *supra* note 76, at 834 (emphasis in original).

82. *See* John Reed, *Chris Soghoian on What's Wrong With the Debate on Section 215*, JUST SECURITY, (June 1, 2015, 2:51 pm), http://justsecurity.org/23369/chris-soghoian-wrong-focusing-section-215/ [https://perma.cc/GB3L-54TB] (decrying lack of technological knowledge informing the surveillance debate).

databases, the querying process, and any algorithms in use, individual FISA judges may not be able to sufficiently understand the technology to perform effective oversight.[83]

FISA judges' need for timely and accurate information regarding how the government is conducting surveillance has unfortunately not been a topic of public discussion. Such information is particularly important to effective gatekeeping—no overseer can assess the government's compliance absent accurate information about what the government is doing. Yet the court has been surprised time and again by aspects of executive-branch collection activities.[84] Failure to address deficiencies in the flow of information to the FISA Court will undermine the success of any other reforms, as the court can only operate effectively if it has all the relevant facts before it.

II. REALITIES OF THE FISA COURT

This Part will review the FISA Court's performance in the context of bulk-collection programs with an eye to whether the preceding criticisms are warranted. It will argue in Part II.A that the FISA Court has taken seriously its role as gatekeeper, engaging in active oversight and at times imposing meaningful checks on executive-branch surveillance activities. Part II.B demonstrates that the court's performance as rule maker, however, has not exhibited similar effectiveness. Instead, the FISA Court's bulk-collection approvals fail to grapple meaningfully with the implications of the government's requests. Moreover, they have uncritically adopted the government's legal arguments, all of which deserve rigorous analysis and some of which are very difficult to square with the relevant statutory text.

A. Strong Gatekeeper Oversight

This Part will detail the ways in which the FISA Court has, contrary to generalized critiques of the court, aggressively exercised its gatekeeping power to oversee FISA programs. The power to impose gatekeeping limits on the government's FISA powers derives from a variety of sources of authorization and can be deployed at multiple points during the course of the application, approval, and implementation process. The most notable source of authority is, of course, Article III of the Constitution, which vests the "judicial Power of the United States" in federal courts.[85] Inherent in this judicial power is a court's equitable power to protect its "proceedings and judgments in the course of discharging [its] traditional responsibilities,"[86] and the FISA Court is no different from any other Article III court in this regard.[87] FISA itself recognizes these inherent powers when it specifies that the statute should not "be construed to reduce or contravene the inherent authority of

---

83. *See* PRESIDENT'S REVIEW GRP. REPORT, *supra* note 43, at 205; Donohue, *supra* note 76, at 821–22 (arguing that the dearth of technological knowledge is similarly problematic when it comes to congressional overseers).

84. *See infra* Part II.A.

85. U.S. CONST. art. III, § 1.

86. Degen v. United States, 517 U.S. 820, 823 (1996).

87. *See In re* Motion for Release of Court Records, 526 F. Supp. 2d 484 (FISA Ct. 2007).

the court . . . to determine or enforce compliance with an order or a rule."[88] The FISA Court Rules of Procedure also reinforce the idea that FISA judges may use their equitable power by providing, for example, that judges may collect any information they deem relevant to carrying out their obligations.[89]

FISA judges have put these equitable powers to work when the government initially applies for surveillance authority, when the government seeks to renew an authority, and in response to government noncompliance. Whether those mechanisms suffice to bar unlawful government activity is a separate, and more debatable, question.[90]

1. Government Applications as Gatekeeping Opportunities

When acting as gatekeeper to the FISA surveillance powers, a critical moment comes at the beginning of the process—the FISA judge's consideration of a government application. The process of applying for a FISA Court order is designed to be much more than a rubber-stamping operation. It is an iterative process in which the presiding judge, members of the FISA Court staff, and government lawyers responsible for preparing applications engage in a dialogue. 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.[91]

When the government seeks approval of a request for targeted, rather than bulk, surveillance, the FISA Court has a clear opportunity to exercise its gatekeeping powers. Just as a magistrate judge examines an application for a search warrant, the

---

88. 50 U.S.C.A. § 1803(h) (West 2015).

89. FISA CT. R. 5(c) ("The Judge before whom a matter is pending may order a party to furnish any information that the Judge deems necessary.").

90. Some critiques of the FISA approval process have identified a concern not addressed in this Article—the infrequency of collateral review of FISA surveillance orders. There is a robust regime available for challenging criminal warrants—an individual can challenge the validity of a warrant by moving to bar the government from introducing at his trial evidence that resulted from the warrant, or by bringing a civil damages claim against the law enforcement officials who carried out the allegedly invalid warrant. FISA orders, by contrast, are much more insulated from collateral attack. First, they are much less likely to lead to criminal prosecution, so the opportunity for a suppression motion is rare. Second, when they do lead to evidence used in a criminal trial, the defendant's ability to challenge their validity has been narrowly constrained by the federal courts. *E.g.*, United States v. Daoud, 755 F.3d 479 (7th Cir. 2014) (limiting defendant's access to FISA materials when challenging an order's validity). Finally, courts have proved hostile to damages claims based on FISA violations. *E.g.*, Al-Haramain Islamic Found., Inc. v. Obama, 705 F.3d 845, 855 (9th Cir. 2012) (holding United States immune from suit asserting violations of FISA). While the paucity of opportunity for collateral review of FISA orders is highly problematic, critiques on this basis are not critiques of the FISA Court's gatekeeping performance. Rather, they are challenges to the lack of mechanisms for challenging FISA Court orders once they have been implemented. *See* GOITEIN & PATEL, *supra* note 21, at 34 (listing the barriers to challenging FISA Court orders).

91. Letter from Hon. Reggie B. Walton, *supra* note 20.

FISA judge examines the government's targeted surveillance application to ensure that it complies with all statutory and constitutional requirements. Indeed, it is this gatekeeping role for which the FISA Court was created. And we have seen the FISA Court operate effectively in this capacity. The FISA Court "twice refused to authorize Section 215 orders [by the FBI] based on concerns that the investigation was premised on protected First Amendment activity."[92] In other words, when the government's proposed surveillance activities threatened the constitutionally protected rights of American citizens, the FISA Court refused to provide authorization.

Perhaps counterintuitively, however, the court engages in gatekeeping activity even in the rule-making context. Take for example the government's application for the collection of Internet data in bulk under FISA's pen/trap provision.[93] In that instance, the court is being asked to make rules—to determine whether the statute can be interpreted to authorize the government's desired activity. It is facing a question of first impression and determining whether the statute's authorization lawfully extends to the new circumstances that the government presents. It is rule making like any common law court. What is less evident is the gatekeeping aspect to this process. Again, the initial bulk Internet collection application is an example. The pen/trap provision provides that the judge must enter an order approving the use of a pen/trap device if the judge finds, inter alia, that the application includes a certification from the government that it is likely to collect foreign intelligence information or is relevant to investigations of international terrorism or clandestine intelligence activities.[94] The government argued that this language meant that "the Court's exclusive function" was "to verify that [the certification] contains the words required" by the statute;[95] in other words, that the provision reduced the approving judge's role to that of ensuring the government had checked off all the required boxes. FISA Judge Colleen Kollar-Kotelly was concerned, however, about the breadth of the collection contemplated by the proposed authorization and rejected the government's view on this point. She refused to concede that "FISA prohibits the Court from engaging in any substantive review of [the government's] certification."[96] "*[A]uthorizing* the Court to issue an order when a certification is made," she pointed out, "and *requiring* it to do so without resolving doubts about the correctness of the certification, are quite different."[97] So despite statutory language that arguably

---

92. OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006, at 73 (2008). The FBI subsequently issued National Security Letters (NSLs) to obtain this information built on the same premise rejected by the court, thereby executing an end run around the court. *Id*. NSLs are administrative subpoenas that the government can use to demand information without judicial approval. *See* 18 U.S.C.A. § 2709 (West 2015).

93. *See infra* Part II.B.1.

94. 50 U.S.C.A. § 1842(c)(2) (West 2015).

95. Judge Kollar-Kotelly's Pen/Trap Opinion, *supra* note 54, at 26.

96. *Id.* at 26; *see also* Memorandum Opinion at 8 n.10, *In re* [REDACTED], No. PR/TT [REDACTED] (FISA Ct. 2010) [hereinafter Bates Memorandum Opinion] (reauthorizing bulk collection of Internet metadata under FISA's pen/trap provision).

97. Judge Kollar-Kotelly's Pen/Trap Opinion, *supra* note 54**,** at 27 n.19 (emphasis in original).

requires otherwise, the FISA judge reserved the right to look behind a government certification to assess whether its contents were accurate. In other words, separate and apart from making a new rule authorizing bulk collection under the pen/trap statute, the court used the order in which that rule was first announced as an opportunity to engage in gatekeeping as well, insisting on making an independent determination of whether the government had satisfied the requirements of that newly minted rule.

2. Information as a Gatekeeping Tool

A tool that FISA judges often have put to use in their efforts at ongoing oversight is the authority to demand additional information from the government at all stages of the application and renewal process. Some of the court's demands for information in the rule-making role are explicitly designed to facilitate subsequent gatekeeping. When setting out the parameters of the government's new authority, the court often includes in its orders provisions that ensure that it will continue to receive information about the government's activities—thereby allowing ongoing oversight—even after a surveillance order has been issued. To this end, judges have sometimes imposed specific, extrastatutory information-sharing prerequisites for reauthorization of a particular order. In her original order authorizing the pen/trap bulk-collection program, for example, Judge Kollar-Kotelly specified that each government application for reauthorization had to include "a report discussing queries that have been made since the prior application," as well as the NSA's application of court-imposed limits on the use of the information.[98] Similarly, the FISA Court's orders have always required that any renewal application for the section 215 bulk telephony-metadata collection "include a report on the implementation of the Court's prior orders."[99]

At other times, the use of information requests is retrospective. This was true, for example, of demands for additional information that came in response to several instances in which the NSA failed to comply with various FISA Court orders. These instances of noncompliance—frequently long-standing and systemic noncompliance—do not appear to have been the result of intentional misconduct; they have been significant nonetheless. One such instance came in the context of Judge Reggie Walton's oversight of the government's use of both the telephone metadata and the pen/trap databases. The FISA Court's orders authorizing these bulk-collection programs required that an NSA official determine that there was "reasonable articulable suspicion" that any seed identifier used to query the database is "associated with" a particular terrorist organization.[100] This requirement is known as the "RAS standard." In early January 2009—more than three years after the program was initiated—Justice Department officials learned that the NSA had

---

98. *Id.* at 86.

99. *E.g.*, Order at 6, *In re* Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. March 2, 2009) [hereinafter March 2, 2009, Order].

100. Judge Kollar-Kotelly's Pen/Trap Opinion, *supra* note 54, at 83–84; *see also* Order Regarding Preliminary Notice of Compliance Incident Dated January 15, 2009 at 2, *In re* Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Jan. 28, 2009) [hereinafter Jan. 28, 2009, Order] (describing the RAS standard).

regularly queried the telephony metadata database using seeds that had not been deemed to meet the RAS standard.[101] As it turned out, "nearly ninety percent of the queries to the bulk dataset" up to that point had used non-RAS-approved numbers.[102] Compounding the problem, the NSA had, in its regular reauthorization applications, consistently provided the FISA Court with an inaccurate description of this querying process.[103] As Judge Walton subsequently pointed out, this meant that "since the earliest days of the [FISA Court]-authorized collection of call-detail records by the NSA, the NSA ha[d] on a daily basis" used the database in a manner "prohibited by the governing minimization procedures under each of the relevant Court orders."[104]

In response to the government's "flagrant violation[s]" of the FISA Court's orders, Judge Walton ordered the government—through declarants "of sufficient stature that they have the authority to speak on behalf of the Executive Branch"—to provide detailed information about the telephony metadata program.[105] In particular, he sought the government's input "to help the Court assess whether the Orders issued in this docket should be modified or rescinded; whether other remedial steps should be directed; and whether the Court should take action regarding persons responsible for any misrepresentations to the Court or violations of its Orders."[106] In addition, the order posed specific questions about the program and the related compliance incidents for the government to answer, such as who was responsible for the noncompliance, how long it went on, how it was discovered, and why existing oversight mechanisms failed to identify the problem earlier.[107]

In addition, recognizing that the pen/trap metadata program operated in a similar manner, Judge Walton proactively asked the government to investigate whether the same problems also existed with respect to the pen/trap data. As it turned out, the pen/trap metadata had also been queried using non-RAS-approved seeds.[108]

In response to these January 2009 discoveries, Judge Walton required the government to provide him with a report on the results of an "end-to-end review" of NSA's handling of bulk-collection material.[109] Judge Walton's order specified that the report should include any additional noncompliance that was discovered as a result of the end-to-end review, "discussion of the steps taken to remedy . . . non-compliance," and "minimization and oversight procedures the government propose[d]" to apply to the program going forward.[110]

Additional compliance problems prompted the court to employ even more assertive gatekeeping information demands. In addition to its failure to comply with the RAS standard, the NSA also reported improper access to the telephony metadata

---

101. *See* Jan. 28, 2009, Order, supra note 101, at 2.

102. Donohue, *supra* note 76, at 811–12.

103. Supplemental Declaration of Lieutenant General Keith B. Alexander at 16–19, *In re* Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 25, 2009) [hereinafter Declaration of Lt. Gen. Alexander].

104. March 2, 2009, Order, *supra* note 100, at 4–5.

105. Jan. 28, 2009, Order, *supra* note 101, at 4–5.

106. *Id.* at 2.

107. *Id.* at 2–4.

108. *See* Bates Memorandum Opinion, *supra* note 97, at 15.

109. *E.g.*, Declaration. of Lt. Gen. Alexander, *supra* note 104, at 2.

110. March 2, 2009, Order, *supra* note 100, at 20.

database[111] and failure to comply with FISA Court orders regarding the use and dissemination of information gathered through the bulk-collection programs.[112] To address the violation of dissemination rules, the court insisted on a weekly reporting requirement. Every seven days, the NSA was obligated to submit to the FISA Court a list of each incidence of dissemination of information outside the NSA from the metadata databases for the preceding week.[113] And because its previous efforts to ensure compliance had not succeeded in preventing unauthorized dissemination of database information, the FISA Court took more drastic information-collection action in that context as well.[114] Not satisfied in this instance with demanding a written submission, Judge Walton required NSA and the Justice Department's National Security Division officials to appear for a hearing "to inform the Court more fully of the scope and circumstances of the incidents" and "to allow the Court [to] assess whether the Orders issued in this docket should be modified or rescinded and whether other remedial steps should be imposed."[115] At this hearing, Judge Walton ordered the government to submit a report explaining how it had handled the compliance issues that had been discovered.[116] Not satisfied with the level of detail

---

111. Improper access to the telephony metadata database had been a persistent problem. *Id.* at 9 (over two dozen analysts had queried the telephony metadata database for several days in April 2008 "without being aware they were doing so" (emphasis omitted)); Donohue, *supra* note 76, at 815. NSA responded by "suspending . . . access pending additional training" and changing the access tool to require acknowledgment of access to metadata. March 2, 2009, Order, *supra* note 100, at 9–10. An audit revealed that as late as February 2009 analysts continued to query the records using seeds that were not RAS-approved. *Id.* at 10; Declaration of Lt. Gen. Alexander, *supra* note 104, at 8; PCLOB SECTION 215 REPORT, *supra* note 34, at 51.

112. In June 2009, the government reported to the court that the "unminimized results of some queries of metadata [redacted text] had been 'uploaded [by NSA] into a database to which other intelligence agencies . . . had access,'" which "may have resulted in the dissemination of U.S. person information in violation" of minimization policy as well as the Court's orders. Order at 5, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 09-06 (FISA Ct. June 22, 2009) [hereinafter FBI Application Order] (alteration in original) (describing May 29, 2009 order).

113. *Id.* at 7. This requirement was later relaxed to every thirty days. *See* Bates Memorandum Opinion, *supra* note 97, at 95.

114. One NSA analyst, for example, forwarded the results to other NSA analysts, at least some of whom had not received "appropriate and adequate briefings" about the relevant restrictions on the use and dissemination of the metadata. Order Regarding Further Compliance Incidents at 3, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 09-13 (FISA Ct. Sept. 25, 2009) [hereinafter FBI Application Further Compliance Order] (internal quotation marks omitted). Coming on the heels of a purportedly thorough review of the section 215 program, these revelations "deeply troubled" the court. *Id.* at 4.

115. *Id.*

116. Supplemental Opinion and Order at 6–7, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 09-15 (FISA Ct. Nov. 5, 2009) [hereinafter FBI Application Supplemental Order]. Telephony metadata was disseminated to analysts not trained to receive it, and analysts had queried the database using selectors for which there had been, but was no longer, RAS. *Id.* at 3–4.

provided in that initial report, the judge required yet another report, this time specifying particular information that it must include.[117]

So FISA judges have been quite diligent in seeking information about the bulk-collection programs they are overseeing, particularly when they learn of instances in which the government acted in violation of their orders. This information seeking itself aids in the court's gatekeeper duties. Asking the government to provide information sends a clear signal that the court is paying attention. It also forces the government to be more diligent in its implementation of the court's orders. But the FISA Court does not limit its gatekeeping activity to collecting information. It goes on to make use of the information gleaned from these demands to address concerns that the information reveals.

3. Other Gatekeeping Tools

There are other tools the judges have used to either facilitate or engage in gatekeeping. One is to require minimization or "minimization-like" procedures. While section 215 has always statutorily required the government to employ appropriate minimization procedures, the same was not true of FISA's pen/trap provision prior to the passage of the USA FREEDOM Act.[118] Yet the FISA Court imposed mandatory minimization-like procedures on this data anyway, as a safeguard for concerns arising from the breadth of the collection.[119] These minimization-like procedures included, inter alia, an enhanced oversight role for the NSA's Office of the General Counsel as well as requirements that the NSA label the data as bulk collected, make it available only to trained analysts, and query the database only on seeds that meet the RAS standard.[120]

Enhanced minimization was also the FISA Court's means of remedying overcollection under section 702 of the FISA Amendments Act.[121] Section 702 permits the collection of the content of electronic communications so long as the target of the surveillance is "reasonably believed to be located outside the United States."[122] Due to the technical means by which communications traverse the Internet, however, the NSA was collecting vast numbers of purely domestic communications.[123] The scope of this domestic collection, the FISA Court held, exceeded the authority conferred by statute and violated the Fourth Amendment.[124]

---

117. *Id.* at 6–7.

118. USA FREEDOM Act of 2015, Pub. L. No. 114-23, sec. 202, § 402(a), 129 Stat. 268, 277–78 (to be codified at 50 U.S.C. § 1842) (adding a requirement that the Attorney General "safeguard nonpublicly available information concerning United States persons that is collected through the use of a [pen/trap device]").

119. Judge Kollar-Kotelly's Pen/Trap Opinion, *supra* note 54, at 68, 82–87; *see also* Bates Memorandum Opinion, *supra* note 97, at 82.

120. Judge Kollar-Kotelly's Pen/Trap Opinion, *supra* note 54, at 69 n.50, 83–85.

121. *See* Memorandum Opinion at 16 n.14, *In re* [REDACTED], No. [REDACTED] (FISA Ct. Oct. 3, 2011) [hereinafter Oct. 3, 2011, Memorandum Opinion] (noting the government's repeated substantial misrepresentations of its collection programs).

122. 50 U.S.C. § 1881a(a) (2012).

123. Oct. 3, 2011, Memorandum Opinion, *supra* note 122, at 16 n.14, 33–35.

124. *Id.* at 62–63, 78–79.

To bring the program into compliance with the statute and the Constitution, Judge Bates insisted that the government augment its minimization efforts with respect to this material, and he refused to reauthorize the program until he had approved the government's amended minimization procedures.[125]

Restricting collection and dissemination decisions to a limited roster of properly trained officials is another tactic the court has invoked. Both the initial determination that RAS exists for a particular seed and the determination that minimization requirements have been met before any metadata is disseminated must be made by one of a small number of specified officials.[126] In addition, upon discovering the NSA's longstanding failure to comply with the rules regarding the dissemination of U.S. person information, the court insisted that NSA employees responsible for handling this sensitive information undergo supplemental training with respect to the applicable rules.[127]

An oversight measure that has proved effective in preventing systemic overcollection or overdissemination is that of requiring periodic spot checks. An early noncompliance incident in the pen/trap bulk-collection program prompted the court to impose requirements that the Justice Department's National Security Division and the General Counsel of the NSA spot check of sample data, "at least twice during the 90-day authorized period of surveillance," to be sure the program complied with court requirements.[128] At least once, both of those offices also had to review a sample of the RAS approvals for selection terms. And the NSA had to regularly provide the FISA Court with a report detailing the queries made since the last report submitted to the court, describing the NSA's implementation of procedures to access the metadata and any proposed changes in the collection or use of the metadata.[129] To facilitate these sorts of periodic checks, the FISA Court has required an auditable record of NSA access to bulk-records databases.[130] One of these spot checks revealed that, from the time of the bulk-pen/trap program's initial authorization in 2004, certain "categories" of information not authorized for collection were nonetheless collected continuously.[131] The problem eluded detection by the NSA's end-to-end review or any other oversight mechanism. It was only

---

125. *Id*. at 29, 79–80 (describing modifications to minimization procedures).

126. Primary Order at 6–9, 13, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 09-13 (FISA Ct. Sept. 3, 2009) [hereinafter Sept. 3, 2009, Primary Order].

127. *Id.* at 14–15.

128. Bates Memorandum Opinion, *supra* note 97, at 13 (citation and internal quotation marks omitted); *see also* Sept. 3, 2009, Primary Order, *supra* note 127, at 16 (describing limits).

129. Sept. 3, 2009, Primary Order, *supra* note 127, at 18. Initially, this report was required when the government applied for reauthorization of the program; eventually, it was required every 30 days. Primary Order at 16, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 13-80 (FISA Ct. Apr. 25, 2013) [hereinafter Apr. 25, 2013, Primary Order].

130. *E.g.*, Judge Kollar-Kotelly Pen/Trap Opinion, *supra* note 54, at 83. Access to bulk telephony metadata "for foreign intelligence analysis purposes" must also include an auditable record. Apr. 25, 2013, Primary Order, *supra* note 130, at 7.

131. Bates Memorandum Opinion, *supra* note 97, at 20–22.

through the FISA Court–imposed spot-checking requirement that the overcollection finally came to light in 2010 and was remedied.

The most intrusive oversight tool that a FISA judge has employed was the complete suspension of a program absent judicial approval of each individual query. When it became clear to Judge Walton that the problem of querying the bulk records databases using non-RAS-approved seeds was a systemic one, he barred the NSA from running unsupervised queries altogether.[132] From March until September of 2009, Judge Walton ordered that the government seek judicial approval for each individual query of the telephony metadata.[133] Under these rules, the NSA could only access metadata "through a motion that the Court authorize querying of the BR metadata for purposes of obtaining foreign intelligence on a case-by-case basis [that identifies] the telephone identifier for which access is sought [and] provide[s] the factual basis for the NSA's determination that the [RAS] standard has been met."[134] After the NSA completed its end-to-end review, Judge Walton discontinued this requirement and reauthorized the bulk-collection program, subject to a series of more detailed conditions on the information's collection and use.[135]

From September 2009 until the President ordered modifications to the program in the wake of Edward Snowden's information leak,[136] the orders reauthorizing bulk collection of telephony metadata also incorporated the lessons the court had learned. As a result, the program was subject to a spectrum of controls and oversight requirements. Many of the procedures were simply designed to ensure compliance with the applicable rules. So the NSA was instructed to maintain procedures to control access to and use of the metadata, to provide adequate briefings and training to personnel authorized to receive query results, and to implement software controls both to limit and to track all access to the metadata.[137]

Finally, the court enlisted other government agencies to assist in its gatekeeping role in the section 215 program. For example, the NSA was required to provide the National Security Division with copies of its procedures, briefing, and training materials;[138] to consult with the National Security Division about any legal opinions about the interpretation, scope, and/or implementation of this authority;[139] and to meet with the National Security Division and any other appropriate NSA officials to assess compliance, submitting in writing to the court the results of that meeting.[140] The NSA Office of the Inspector General was required to have a similar meeting with the National Security Division to discuss oversight and assess compliance.[141] Prior to 2011 when the bulk collection of pen/trap information was discontinued, the

---

132. *Id*. at 15 n.17 (discussing Judge Walton's order).

133. March 2, 2009, Order, *supra* note 100, at 18.

134. *Id.* at 18–19

135. *See* Sept. 3, 2009, Primary Order, *supra* note 127, at 2–3, 5–18.

136. *See* Remarks on United States Signals Intelligence, *supra* note 35, at 6–7 (limiting use of metadata collected under section 215 and calling for the development of an approach that can achieve the program's goals without the government holding this metadata itself).

137. Sept. 3, 2009, Primary Order, *supra* note 127, at 11–12.

138. Sept. 3, 2009, Primary Order, *supra* note 127, at 11, 17.

139. *Id.* at 16.

140. *Id.* at 17.

141. *Id.*

orders reauthorizing that program contained similarly detailed and extensive oversight mechanisms. None of this is to say that the protections were sufficient or that the program should have been continued. It is merely to say that the FISA Court's performance in this regard has been much more than a rubber stamp for the government.

One might argue that, rather than demonstrating the FISA Court's virtues as a gatekeeper, the forgoing instead shows that despite all of the FISA Court's oversight efforts, the government continued to violate its orders, to engage in overcollection, and to access and improperly disseminate metadata information. Moreover, one might opine that the FISA judges should have more severely restricted surveillance programs when government noncompliance came to its attention.

To be sure, the FISA Court did not prevent all problems; as gatekeeper it can only do so much. At the same time, it is clear that no matter the outcome, the FISA Court took seriously its responsibility to engage in oversight, took action to press the government to comply with its orders, and served as a partner in devising means of permitting the government to continue its surveillance activities without abdicating all limits and controls. In addition, through its demands for information, spot checks, and other methods, the FISA Court ended noncompliance that might otherwise have continued unchecked, prompted examinations of the system that revealed to additional flaws, and led to the implementation of measures that should lead to better compliance going forward.

B. Weak Rule-Maker Analysis

Given the secret, nonadversarial nature of the pre-USA FREEDOM Act FISA Court's operations, it should perhaps come as no surprise that FISA judges have been insufficiently rigorous in their rule making about bulk-collection programs. While the FISA Court does have its defenders, the verdict of independent committees, government agencies, federal courts, and legal commentators is nearly unanimous in finding FISA Court "rule making" opinions regarding bulk collection wanting.[142] Indeed, even those who endorse the opinions' conclusions refrain from defending their reasoning.[143] The opinions sometimes fail to grapple with the difficult legal questions that are presented and sometimes seem to adopt uncritically the government's arguments, even when those arguments call for serious analysis. These flaws are on display in the initial opinions authorizing the bulk collection of information through the FISA pen/trap and business records provisions respectively.

---

142. *See, e.g.*, ACLU v. Clapper, 785 F.3d 787, 815–19 (2d. Cir. 2015) (holding that the section 215 program was not authorized by the statutory language); Klayman v. Obama, 957 F. Supp. 2d. 1, 29–42 (D.D.C. 2013 (arguing that the section 215 program was likely unconstitutional), *vacated*, 800 F.3d 559 (D.C. Cir. 2015); PCLOB SECTION 215 REPORT, *supra* note 34, at 57–136 (describing in detail multiple arguments that the FISA court's analysis was flawed); PRESIDENT'S REVIEW GRP. REPORT, *supra* note 43, at 203–04; Donohue, *supra* note 76, at 822–24 (lamenting the precedential value assigned to FISA Court opinions).

143. *E.g.*, PCLOB SECTION 215 REPORT, *supra* note 34, at 208–18 (dissenting views by members of the PCLOB); Margulies, *supra* note 59, at 52–53.

1. Authorizing Bulk Collection of Internet Metadata

As discussed in Part I.A.2, Judge Kollar-Kotelly wrote the opinion in 2004 approving for the first time the collection of domestic Internet-communications metadata under the statutory provision authorizing the use of pen/traps.[144] And while she was a strong gatekeeper—insisting on a role in evaluating the government's submissions, demanding additional information about First Amendment implications, and imposing restrictions on the use of the collected data[145]—her rule-making performance was less impressive. Indeed, her opinion sidesteps the truly thorny questions that the bulk-collection application presents.

The opinion notes at the very outset that the government's application sought "a much broader type of collection than other pen register/trap and trace applications."[146] The FISA pen/trap provision in effect at the time required the FISA Court to approve a pen/trap application whenever the Attorney General certified "that the information likely to be obtained . . . is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities."[147] Its plain text indicates that the pen/trap statute envisioned collection of metadata information from individual targets. One clue to the statute's intended use came in the provision indicating what must be included in a FISA judge-issued pen/trap order:

> An order issued under this section . . . shall specify . . . the identity . . . of the person who is the subject of the investigation[,] the identity . . . of the person . . . in whose name is listed the [targeted facility] . . . [and] the attributes of the communications to which the order applies.[148]

Yet the government sought authorization to utilize this provision not to collect noncontent information about a particular subscriber's communications but instead to engage in bulk collection of "specified [classified] categories of metadata about Internet communications."[149] In other words, rather than collecting the e-mail addresses with which Suspect X corresponded, the government sought to collect an entire category of noncontent data—for example, all noncontent data about e-mail traffic into and out of the United States.[150]

Judge Kollar-Kotelly displayed obvious misgivings regarding the application of the statutory provision urged by the government. Recall that the statute provided that when the Attorney General makes the required certification that use of a pen/trap is

---

144. For a definition of metadata, *see supra* note 2.

145. *See supra* text accompanying notes 100–01.

146. Judge Kollar-Kotelly's Pen/Trap Opinion, *supra* note 54, at 1–2.

147. 50 U.S.C. § 1842(c)(2) (Supp. 2003). This provision was modified by the USA FREEDOM Act of 2015. Pub. L. No. 114-23, 129 Stat. 268 (codified in scattered sections of the U.S.C.).

148. 50 U.S.C. § 1842(d)(2) (Supp. 2003) (modified by the USA FREEDOM Act of 2015).

149. Bates Memorandum Opinion, *supra* note 97, at 2. The list of what categories were approved for collection is not available publicly, but at the very least they include IP addresses and e-mail addresses.

150. The actual categories of data that the government collected remain classified.

likely to yield information "relevant to an ongoing investigation,"[151] "the judge shall enter an ex parte order."[152] That is to say, the statute seems to insist that once the government certifies that the relevance standard is met, the FISA judge (so long as all other requirements are also met) has no discretion with respect to whether to issue an order.[153] But the opinion rejects the seemingly self-evident conclusion that the statute eliminates an independent role for the court in evaluating the sufficiency of the government's certification. Clearly uncomfortable with giving such broad collection authority to the government without judicial oversight, Judge Kollar-Kotelly insists that the Court is permitted to look behind the government's certification to "resolv[e] doubts about the correctness of the certification."[154]

Perhaps more revealing of Judge Kollar-Kotelly's concerns are the procedural limitations she imposed on the program. Unlike section 215, the pen/trap provision at the time did not require minimization procedures.[155] Yet Judge Kollar-Kotelly imposed them nonetheless, placing restrictions on storage, access, and dissemination of the collected metadata. The specific restrictions were nearly identical to the minimization procedures statutorily imposed on the section 215 bulk-collection program.[156]

Imposing these minimization procedures demonstrates that Judge Kollar-Kotelly saw the pen/trap bulk collection as severely intrusive into individual privacy rights. Minimization procedures developed in response to concerns that collection, use, or dissemination of some Fourth Amendment-protected material would be unconstitutionally intrusive without such measures. For example, courts considering the constitutionality of FISA content-collection provisions have relied, at least in part, on minimization procedures to conclude that the collection is "reasonable" and

---

151. 50 U.S.C. § 1842(c)(2) (Supp. 2003).

152. 50 U.S.C. § 1842(d)(1) (2000). Arguably, the very fact that the statute confers such little control over the power on judges is evidence of Congress's intent to authorize collection that was narrow in scope. *See* Orin Kerr, *Problems with the FISC's Newly-Declassified Opinion on Bulk Collection of Internet Metadata*, LAWFARE (Nov. 19, 2013, 2:35 AM), https://www.lawfareblog.com/problems-fiscs-newly-declassified-opinion-bulk-collection-internet-metadata [https://perma.cc/XZ7F-PB72].

153. *Cf. In re* Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 846 F. Supp. 1555, 1561–62 (M.D. Fla. 1994) (interpreting the domestic criminal pen/trap statute to foreclose additional judicial inquiry once the government's application has met the statutory requirements). *But see* Judge Kollar-Kotelly's Pen/Trap Opinion, *supra* note 54, at 27 n.19.

154. Judge Kollar-Kotelly's Pen/Trap Opinion, *supra* note 54, at 27 n.19.

155. The USA FREEDOM Act of 2015 added a minimization requirement to the pen/trap provision. Pub. L. No. 114-23, sec. 202, § 402, 129 Stat. 268, 277–78 (codified at 50 U.S.C. § 1842).

156. Judge Kollar-Kotelly's Pen/Trap Opinion, *supra* note 54, at 82–87 (requiring in part that the information remain segregated, that limited numbers of people have access to the information, that the relevant database be queried only using seeds meeting the RAS standard, that any queries be auditable, that the NSA's General Counsel monitor the program, and that any dissemination comply with existing rules about minimizing U.S. person information).

therefore consistent with the Fourth Amendment.[157] In other words, absent the use of minimization procedures to mitigate the privacy impact of collecting Fourth Amendment-protected "papers and effects," FISA content collection might impermissibly intrude on Fourth Amendment rights.

If, however, noncontent data such as the information collected pursuant to the pen/trap statute is not protected by the Fourth Amendment—as the government maintains and Judge Kollar-Kotelly accepts—the "reasonableness" requirement is simply inapplicable.[158] There is no constitutional reason to minimize the information gathered from such collection. Of course Congress can add statutory privacy protections that exceed the Fourth Amendment floor. The minimization procedures imposed on section 215 represent one such regulation. But these limits derive from a congressional determination that constitutional protections are insufficient. Congress could have imposed minimization procedures on pen/trap collection as a means of limiting its privacy impact despite the inapplicability of the Fourth Amendment just as it did for section 215 collection. But it did not. If Judge Kollar-Kotelly found the government's intended use of the pen/trap provision in need of protections often employed for Fourth Amendment-protected information, perhaps she should have concluded that the government's interpretation of what the statute permits is broader than Congress intended.

Judge Kollar-Kotelly's analysis of whether the government's application met the statute's requirement that the information collected be "relevant" to an ongoing investigation also displays her qualms that the pen/trap provision, as interpreted by the government, was excessively broad. Accepting that "only a very small percentage of the information obtained will be . . . directly relevant," Judge Kollar-Kotelly found the bulk collection to be relevant nonetheless because "the collection of both a huge volume and high percentage of unrelated communications [is] necessary to identify the much smaller number" of terrorism-related communications.[159] Consequently, she concluded, the applicable relevance standard did 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 [redacted] FBI investigations."[160] In other

---

157. *E.g.*, *In re* Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1013 (FISA Ct. Rev. 2008); United States v. Rosen, 447 F. Supp. 2d 538 (E.D. Va. 2006).

158. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding that the Fourth Amendment does not apply to the list of phone numbers one dials). The third-party doctrine that the Supreme Court created in a series of opinions in the 1970s, including *Smith*, *see infra* notes 184–93 and accompanying text, provides that information voluntarily revealed to a "third party," a term encompassing any individual or non-government institution, enjoys no Fourth Amendment protection. *See generally Smith*, 442 U.S. 735; United States v. Miller, 425 U.S. 435 (1976). The doctrine arguably applies not only to communications metadata but also banking and medical records, Amazon shopping history, etc. And while the doctrine has been subject to significant criticism, from both courts and commentators, *see, e.g.*, United States v. Jones, 132 S. Ct. 945, 954–57 (2012) (Sotomayor, J., concurring); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 n.5 (2009) (listing some of the critiques of the doctrine), it is clear that Judge Kollar-Kotelly accepted its applicability to the pen/trap metadata.

159. Judge Kollar-Kotelly's Pen/Trap Opinion, *supra* note 54, at 48–49.

160. *Id.* at 49–50.

words, even though the vast majority of the information collected under the pen/trap program will not actually be relevant to a terrorism investigation, the government can only find the information that is relevant if it collects large volumes of information. Therefore, the entire database is relevant.

To support this conclusion, Judge Kollar-Kotelly indicates that she "finds instructive Supreme Court precedents on when a search that is not predicated on individualized suspicion may nonetheless be reasonable under the Fourth Amendment."[161] Those precedents establish a balancing test for evaluating "reasonableness," in which courts must weigh the privacy expectations of the individual and the intrusiveness of the search against the government's interest.[162] Despite noting that she does not consider the pen/trap metadata subject to Fourth Amendment protections, Judge Kollar-Kotelly goes on to employ this balancing test as part of her inquiry into whether the metadata is relevant to an ongoing investigation. She determines that the privacy interest is minimal given the absence of Fourth Amendment protection, and the government interest in thwarting terrorist attacks is compelling. And because the proposed bulk collection is analogous to suspicionless searches that have been upheld under the Fourth Amendment, the determination that the information is relevant is appropriate, despite the fact that only a very small proportion of the huge volume of information will actually be directly relevant.[163]

In other words, despite the inapplicability of the Fourth Amendment to the data collected, Judge Kollar-Kotelly determines that the information collected under the pen/trap bulk-collection program is "relevant" to a qualified investigation because it satisfies the balancing test that would apply to information protected under the Fourth Amendment.[164] But this is a non sequitur. The statutory meaning of the word "relevance" is not contingent on whether a program would be considered constitutional if the Fourth Amendment applied. The question is whether Congress has authorized this use of the pen/trap statute. The opinion never explains what applicability a Fourth Amendment balancing test has on whether the information in question satisfies the "relevant" requirement.

If the government's desired use of an authority seems inconsistent with the level of judicial oversight contemplated by the statute, a reasonable judge might conclude the statute does not actually permit that use, rather than concluding that the statute does not mean what it says. But Judge Kollar-Kotelly reached the opposite conclusion, approving the government's use of the pen/trap statute, but only after asserting a more aggressive judicial oversight role and imposing minimization-like procedures on the resulting information.[165]

---

161. *Id.* at 50.

162. *Id.* at 50–52.

163. *Id.* at 54.

164. *Id.*

165. During the seven years that the pen/trap bulk-collection program continued, there is no indication that any FISA judge analyzed independently this interpretation of the pen/trap provision. In the wake of compliance problems, Judge John Bates imposed additional oversight mechanisms—beefed up the gatekeeping—but did not revisit the substantive analysis. Bates Memorandum Opinion, *supra* note 97, at 82–97.

2. Authorizing Bulk Collection of Telephony Metadata

The FISA Court's approval of the telephony metadata collection under the pre-USA FREEDOM Act version of section 215 also displays questionable legal analysis and has been roundly criticized. In fact, a majority of the members of the PCLOB determined that, contrary to the FISA Court's conclusion, "there are multiple and cumulative reasons for concluding that Section 215 does not authorize the NSA's ongoing daily collection of telephone calling records concerning virtually every American."[166] This Part does not purport to provide an exhaustive list of the grounds on which the FISA Court's approval may be (and has been) assailed.[167] It will, however, briefly note some of the most problematic aspects of the FISA Court's analysis and devote some attention to a few less well-trodden arguments.

First and foremost, it seems that no FISA judge undertook the project of actually putting to paper the legal justification for the program until after news of it had leaked to the public. From 2006 to 2013, the FISA Court permitted the NSA to collect all telephony metadata without (apparently) bothering to draft a reasoned opinion explaining why the program was within the government's statutory authority. The government, to be sure, did submit a lengthy brief to the court setting out its own arguments for the lawfulness of the program.[168] But the order approving the application was issued the day after the government's brief was filed with the court.[169] This did not give the FISA judge a great deal of time to reach a considered decision. Of course, given that FISA Court applications are often the culmination of a series of communications between the Justice Department and the judge, the judge likely knew of the government's arguments before they were officially filed.[170] And one must assume that the FISA Court was convinced by those arguments. Nevertheless, while the initial approval of the pen/trap bulk Internet data collection program called for an eighty-seven-page memorandum opinion,[171] the interpretation of a different statutory provision to permit equally expansive collection of phone records merely produced an order stating that the government's application satisfied section 215's statutory requirements and setting out some (statutorily required)

---

166. PCLOB SECTION 215 REPORT, *supra* note 34, at 57. Two of the PCLOB's five members disagreed, arguing that, given the complexity of the legal questions presented, the FISA Court's interpretation could not definitively be labeled incorrect; it does not assert that the FISA Court's is the best interpretation of the statute. *Id.* at 210, 215.

167. In addition to the arguments laid out here, see also ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015) (rejecting the government's assertion that the entirety of domestic telephony metadata was "relevant" to an investigation, as required by the statute); PCLOB SECTION 215 REPORT, *supra* note 34, at 57–102 (detailing why the Board concluded that the program was neither authorized by statute nor consistent with the Constitution); Donohue, *supra* note 76, at 836–62 (same).

168. Memorandum of Law in Support of Application for Certain Tangible Things for Investigations to Protect Against International Terrorism, No. BR 06-05 (FISA Ct. May 23, 2006) [hereinafter May 23, 2006, Memorandum of Law].

169. Order, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 06-05 (FISA Ct. May 24, 2006) [hereinafter May 24, 2006, Order].

170. Letter from Hon. Reggie B. Walton, *supra* note 20, at 2–3.

171. Judge Kollar-Kotelly's Pen/Trap Opinion, *supra* note 54.

minimization procedures governing the NSA's storage and use of the resulting data.[172]

The FISA Court did not decline to prepare a written opinion at the inception of the section 215 bulk collection program because the question was an insignificant one. Indeed, the government's application recognized the importance of its request, providing the court with a detailed argument for the legality of using section 215 for bulk collection. That the PCLOB as well as at least one federal judge and one federal appeals court have determined that the program was not consistent with either the Constitution or the language of section 215 (or both) illustrates that at the very least the application presented the court with difficult legal questions on which reasonable minds might disagree.[173] Such questions merit a thorough, reasoned judicial analysis.

Once Snowden revealed the existence of the section 215 program, the FISA Court did issue an opinion. That opinion, however, came out of a government application that differed from its 2006 counterpart in two interesting ways. First, in July 2013, just over a month after Snowden's initial revelations, the government notified Judge Eagan during an ex parte hearing regarding the July 2013 reauthorization application that it was working on "an updated legal analysis . . . with regard to the application of Section 215 to bulk telephony metadata collection."[174] A description of that updated analysis was released publicly in *Administration Section 215 White Paper* on August 9, 2013.[175] In it, the government's argument that the entirety of the metadata is "relevant" to an ongoing investigation is significantly altered from its 2006 counterpart. The 2006 version of its argument, consisting of a few paragraphs, largely relied on the claim that, in determining whether bulk metadata meets the relevance standard, "for reasons of both constitutional authority and practical competence," the court should defer "to the fully considered judgment of the executive branch in . . . determining the potential significance of intelligence-related information."[176] Second, nearly four of the original brief's twenty-seven pages are devoted to a section labeled "The Al Qaeda Threat," reminding the court of the events of 9/11 and al-Qaeda's continuing desire to strike at America.[177] Clearly the government relied on the urgency of the threat to help convince a judge to defer to the government's legal interpretation.

The 2013 *Administration Section 215 White Paper* provides a stark contrast on both of these points. First, the government never mentions al-Qaeda or any other terrorist group. Rather than raising the emotional specter of 9/11, it is devoted

---

172. May 24, 2006, Order, *supra* note 170.

173. *See* ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2015); PCLOB SECTION 215 REPORT, *supra* note 34.

174. Amended Memorandum Opinion at 3 n.4, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [REDACTED], No. BR 13-109 (FISA Ct. Aug. 29, 2013) [hereinafter Aug. 29, 2013, Amended Memorandum Opinion].

175. ADMINISTRATION SECTION 215 WHITE PAPER, *supra* note 33. The white paper was released after the government completed its submission to the court, and Judge Eagan did not rely on it. Aug. 29, 2013, Amended Memorandum Opinion, *supra* note 175, at 3 n.4.

176. May 23, 2006, Memorandum of Law, *supra* note 169, at 16–17 (citation omitted) (internal quotation marks omitted).

177. *Id*. at 4–7.

entirely to legal analysis. Second, it offers an elaborate defense of treating metadata as relevant. This defense includes a meticulous effort to analogize the collection of an entire database of phone records to the type of information collection that goes on during civil or criminal discovery, reassurance that the government's definition of relevance does have limits, and an argument that its relevance analysis satisfies not only section 215's requirements but the Constitution's as well.[178] Clearly the government felt that its existing legal analysis supporting the section 215 bulk collection program—the legal analysis the FISA Court accepted in 2006 and under which the program operated for seven years—was insufficient to withstand public scrutiny. So once the seven-year-old program was made public, the government hurried to provide legal analysis. Did the original order accept these relatively weak analyses (in part) because of the severity of the threat? It is impossible to know. But when the Court in 2013 approved the program just as it had for each of the previous government applications, it did so with the benefit of a much more thorough, less emotional, application.

Nevertheless, even this newly minted defense of the program has been roundly criticized. Perhaps the most widely condemned aspect of the 2013 opinion is its interpretation of section 215's "relevance" requirement—a requirement that mimics the language from the pen/trap provision limiting collection to information relevant to an ongoing applicable investigation. In its May 2006 application, the government relied upon what it referred to as the "ground breaking and innovative" decision Judge Kollar-Kotelly had written for the pen/trap program.[179] The FISA Court did not revisit the propriety of Judge Kollar-Kotelly's treatment of the relevance requirement, nor did it discuss whether or how that interpretation of "relevance"— from the entirely distinct context of the pen/trap application—should be affected by the differences between the telephony metadata collection program, which was governed by section 215, and the Internet metadata collection program implemented pursuant to the pen/trap provision, which was the subject of Judge Kollar-Kotelly's original "relevance" analysis.[180] Any thoroughly reasoned discussion of the lawfulness of the bulk collection of telephony data would have to confront this question. If the court did so, it failed to memorialize why it found the analogy to the pen/trap program sufficiently apt. Moreover, as the PCLOB points out, the FISA Court's interpretation means that "if the government develops an effective means of searching through *everything* in order to find *something*, then *everything* becomes relevant to its investigations. The word 'relevant' becomes limited only by the government's technological

178. ADMINISTRATION SECTION 215 WHITE PAPER, *supra* note 33, at 10–15.

179. May 23, 2006, Memorandum of Law, *supra* note 169, at 3. In the publicly available version of this memorandum, identifying information about the "ground breaking and innovative" decision the government relies on is redacted. As the memorandum quotes from Judge Kollar-Kotelly's 2004 opinion, however, it is clearly referring to that opinion.

180. PCLOB SECTION 215 REPORT, *supra* note 34, at 44 (explaining that under the Internet program, records were acquired if they travelled through designated communications channels likely to contain messages of counterterrorism interest; the section 215 program collected *all* telephony metadata). As the FISA Court has recognized, "nearly all of the call detail records collected pertain to communications of non-U.S. persons [and] U.S. persons who are *not* the subject of an applicable FBI investigation." March 2, 2009, Order, *supra* note 100, at 12 (emphasis in original).

capacity to ingest information and sift through it efficiently."[181] Not even the government argued that section 215 permits such expansive collection. Yet the FISA Court did not explain why telephony metadata differs from other information in such a way that its opinion would not apply with equal force to other types of information. Like the PCLOB, other analyses of the section 215 program have determined that the government's definition of relevance was far broader than Congress intended.[182]

There are also several questions a thorough opinion would have addressed that do not appear at all in the 2013 opinion. One is the question whether the government's position that metadata is not protected by the Fourth Amendment remains valid. That position rests on the applicability of the third-party record doctrine, established in a series of cases in the 1970s, including *Smith v. Maryland*, to telephony metadata.[183] In *Smith*, the government had used a pen register to collect the list of phone numbers dialed from a criminal suspect's home phone. When the government sought to enter that information into evidence at trial, the suspect moved to have it suppressed on the grounds that it was collected without a warrant in violation of the Fourth Amendment. The Supreme Court held that the Fourth Amendment did not protect the information because it was information that a telephone subscriber knowingly surrendered to the telephone company, and the subscriber therefore had no reasonable expectation of privacy in it.[184] It is this doctrine upon which Judge Kollar-Kotelly relied in determining that Internet metadata did not enjoy Fourth Amendment protection in 2004,[185] and Judge Eagan in turn relies in part on Judge Kollar-Kotelly's opinion in reaching the conclusion that the same held true in the section 215 context in 2013.[186]

But in relying on Judge Kollar-Kotelly's analysis, Judge Eagan's section 215 opinion never seriously considers whether the *Smith v. Maryland* argument continues to apply with the same force to telephony metadata collected in bulk in 2013 as it did in 2004. As an initial matter, regardless of the year, several courts and commentators have noted that the privacy interest in an individual's telephony metadata and the privacy interest in the same information gathered in bulk might be very different.

This argument had even more force in 2013 than it did in 2004, given both the technological advances that have taken place in storing and analyzing bulk data and the argument Justice Sotomayor made in her concurrence in *United States v. Jones* in 2012.[187] The *Jones* Court held that, by placing a GPS device on a criminal

---

181. PCLOB SECTION 215 REPORT, *supra* note 34, at 62 (emphasis in original); *id.* (similar databases could be compiled with e-mails, bank accounts, debit and credit card use, money orders, vehicle rentals, hotel records, property leases, library borrowing, and websites visited). "This elastic definition of relevance not only proves too much," the PCLOB argues, "but also supplies a license for nearly unlimited governmental acquisition of other kinds of transactional information collection." *Id.*

182. *Compare id.* at 60–81 *with* ACLU v. Clapper, 785 F.3d 787, 812 (2d Cir. 2015).

183. ADMINISTRATION SECTION 215 WHITE PAPER, *supra* note 33, at 19–20.

184. Smith v. Maryland, 442 U.S. 735, 742–44 (1979).

185. Judge Kollar-Kotelly's Pen/Trap Opinion, *supra* note 54, at 58–63.

186. Aug. 29, 2013, Amended Memorandum Opinion, *supra* note 175, at 8–9.

187. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

suspect's car to record his location information twenty-four hours a day for several weeks without a warrant, the government trespassed on private property in violation of the Fourth Amendment.[188] Concurring in the result, Justice Sotomayor argued that the Court should take a closer look at the Fourth Amendment implications of bulk data collection.[189] In fact, she went so far as to suggest that the Court might need to rethink the scope of the third-party doctrine in light of modern technological tools, calling the continued applicability of that doctrine into question, at least in the context of bulk collection.[190] As Sotomayor points out, the government's contemporary data-storage and search capacity means that aggregating data in bulk permits the government to infer significant and intimate information about an individual's lifestyle—religious habits, social circle, medical condition, and more—that it could not infer from one individual's phone records alone.[191] Yet Judge Eagan simply asserts conclusively that "where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*."[192] Nowhere in her opinion does she mention *United States v. Jones*, nor does she try to explain why the courts and commentators who take a contrary position regarding the ways in which bulk data changes the privacy interests at play are incorrect. Judge Eagan is certainly entitled to conclude that the telephony metadata is not protected by the Fourth Amendment because of *Smith v. Maryland* and its progeny. But doing so in a convincing fashion requires acknowledgement of the contrary argument and a reasoned analysis of why that argument is wrong. The 2013 opinion includes neither of these.

There are several other omissions that the PCLOB discusses,[193] including one that demonstrates nicely the challenge of effective rule making for the court. An issue that the FISA Court left unaddressed—for at least two years—was the question of how the limits on sharing metadata covered by the Electronic Communications Privacy Act (ECPA) might impact the legal analysis of section 215.[194] One provision

---

188. *Id.* at 948 (describing facts); *id.* at 950 (discussing the trespass).

189. *Id.* at 957 (Sotomayor, J., concurring).

190. *Id.*

191. *See id.*; Declaration of Professor Edward W. Felten, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-cv-03994) (describing how metadata can reveal a great deal of intimate information about an individual).

192. Aug. 29, 2013, Amended Memorandum Opinion, *supra* note 175, at 9 (italics in original).

193. PCLOB SECTION 215 REPORT, *supra* note 34, at 57–102 (arguing that the FISA Court did not consider whether the government's interpretation of section 215 ran afoul of its requirement for the information sought to be relevant to *an* (as opposed to many) investigation, whether section 215 permits the FISA Court to issue prospective orders for information that does not exist at the time of the order, or whether it was permissible for the NSA to collect, store, and analyze the telephony metadata when section 215 authorizes the records be "made available to" or "received by" the FBI (internal quotation marks omitted)).

194. *See* Supplemental Opinion at 1, *In re* Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Dec. 12, 2008) [hereinafter Dec. 12, 2008, Supplemental Opinion]. ECPA amended an existing statute so that wire taps on telephone calls also applied to electronic data transmitted by computer. Pub. L. No. 99-508, tit. I, 100 Stat. 1848, 1848–59 (1986) (codified at 18 U.S.C. § 2510). The Stored Communications Act

of ECPA specifies an ostensibly exhaustive list of means by which the government may compel a service provider to produce noncontent records.[195] Section 215 orders do not appear on that list. The court's conclusion that the program did not violate ECPA's limitations on disclosure of customer records may or may not be the right one. What is more important is that the FISA Court failed even to consider the question—and therefore whether the service providers and the government were systematically violating ECPA—for years.[196] These unaddressed arguments are the type of thing that one can imagine being raised by opposing counsel in public, adversarial proceedings.

The government argues that, regardless of how the FISA Court might answer a particular question given a blank slate, the court should defer to the government's interpretation of FISA. This might be either because the Justice Department's or the NSA's interpretation of the statute is entitled to some form of deference often extended to agency interpretations of statutory provisions, or because courts generally should defer to the executive on matters of foreign affairs and national security because of its superior information and expertise. And FISA judges have at times accepted this argument.[197] On this view, the preceding critiques are invalid because the FISA Court is correct in adopting the government's interpretation of the law so long as it is within the bounds of reason.

But the traditional arguments for deference are not triggered in the bulk-collection context.[198] First, consider the administrative law doctrine of *Chevron* deference.[199] Under *Chevron*, judges must accept executive branch agencies' interpretations of ambiguous statutes they are tasked with administering so long as that interpretation is reasonable.[200] There are two barriers to affording *Chevron*-like deference to the interpretation of section 215. As an initial matter, it is not clear that Congress has delegated interpretive power to either the Justice Department or the NSA in the way that many executive agencies are tasked with administering statutes.[201] If any entity has been entrusted with a special role in interpreting FISA, it is the FISA Court itself.

---

added prohibitions on access to stored electronic communications to ECPA. Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860–68 (codified at 18 U.S.C. §§ 2701–10).

195. 18 U.S.C. § 2703(c)(1) (2012).

196. *See* PCLOB SECTION 215 REPORT, *supra* note 34, at 91–95.

197. Judge Kollar-Kotelly's Pen/Trap Opinion, *supra* note 54, at 30–31 ("The Court also recognizes that, for reasons of both constitutional authority and practical competence, deference should be given to the fully considered judgment of the executive branch in assessing and responding to national security threats.").

198. *See* Curtis A. Bradley, Chevron *Deference and Foreign Affairs*, 86 VA. L. REV. 649, 659–64 (2000) (listing some the common justifications for deferring to the executive branch in foreign affairs and national security: "the executive branch needs a high degree of flexibility in order to respond to complex and changing world conditions," "decisions in this area tend to be more political than legal in nature," and "the executive branch has much greater expertise and access to information than the courts concerning foreign affairs matters").

199. Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837 (1984).

200. *Id.* at 843.

201. *See* Bradley, *supra* note 199, at 670–71 ("As the Court suggested in *Chevron* and made clearer in subsequent decisions, '[a] precondition to deference under *Chevron* is a congressional delegation of administrative authority.'" (italics in original) (quoting Adams Fruit Co. v. Barrett, 494 U.S. 638, 649 (1990))).

The executive branch is therefore not entitled to deference beyond the persuasiveness of its arguments. Moreover, many critics of the section 215 opinion—and the same would hold true for the pen/trap opinion as well—do not consider section 215 an ambiguous statute. On this view, the plain language of the statute clearly precludes the executive branch's interpretation of the law.[202] *Chevron* does not compel deference to executive interpretations of unambiguous statutes.

The argument for foreign affairs deference is similarly thin. To the extent that the executive's experience, expertise, and information advantages justify judicial deference on matters of foreign policy and national security, those considerations are not implicated here. The question is a purely legal one concerning the meaning of legislation. This is an area where, if any branch is entitled to deference due to its expertise, it is the judiciary. In addition, this is not an area where the executive is acting in the absence of congressional guidance on the issue. Rather, Congress has explicitly interposed the judiciary between the executive and FISA surveillance for the purpose of ensuring independent oversight of executive branch intelligence collection. Thus, unless the executive branch possesses exclusive, unilateral authority over intelligence collection—a position that not even the government takes with respect to section 215—it is proper for FISA judges to engage in independent judicial interpretations of FISA.[203]

In sum, when the FISA Court considers bulk-collection applications, it seems not to push back very hard against the government's arguments.[204] The court has simply lacked the necessary tools to fulfill its newly minted rule-making role. As a result, rather than serving as an independent check on the executive's efforts, the court has served as an enabler. The next Part considers whether there are ways to remedy this state of affairs.

---

202. PCLOB SECTION 215 REPORT, *supra* note 34, at 99–100.

203. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

204. There has been at least one exception. In 2007, FISA Judge Roger Vinson rejected the government's argument that the program known as the Terrorist Surveillance Program, which collected the contents of communications coming into and out of the United States when one party to the communication was believed to be associated with al-Qaeda, was consistent with the government's powers under FISA, Order and Memorandum Opinion at 16, *In re* [REDACTED], No. [REDACTED] (FISA Ct. Apr. 3, 2007) [hereinafter Apr. 3, 2007, Order and Memorandum Opinion], despite a previous FISA judge having approved of the program, Order, *In re* Various Known and Unknown Agents of [REDACTED] Presumed U.S. Persons, No. [REDACTED] (FISA Ct. Jan. 10, 2007) [hereinafter Jan. 10, 2007, Order]. It was Vinson's opinion that prompted the government to go to Congress and seek legislation that ultimately became the FISA Amendments Act of 2008. Just months later, however, Judge Vinson issued an order authorizing essentially the same surveillance pursuant to a new legal theory. Order, [REDACTED], No. [REDACTED] (FISA Ct. May 31, 2007) [hereinafter May 31, 2007, Order]. Under this theory, the specific target authorized for surveillance was al-Qaeda, so whenever the NSA learned of a new al-Qaeda suspect, his communications would be immediately available for collection. *See id.*; Charlie Savage, *Documents Show N.S.A.'s Wiretap Moves Before Congress's Approval*, N.Y. TIMES (Jan. 27, 2015) http://www.nytimes.com/2015/01/28/us/documents-show-nsas-wiretap-moves-before-congresss-approval.html?_r=0 [https://perma.cc/6NAV-6FWB].

III. REFORM

In this Part, I consider ideas for FISA Court reform, including those enacted in the USA FREEDOM Act, in light of the FISA Court's performance as gatekeeper and as rule maker. Part III.A addresses reforms targeting the court's gatekeeping functions and argues that the court's strong showing as a gatekeeper renders efforts designed to address the "rubber stamp" accusation—such as proposals to modify the process by which judges are named to the FISA Court—unnecessary. At the same time, the court's effectiveness as gatekeeper could be amplified by implementing reform in an area that has thus far received insufficient attention: ensuring that FISA judges have accurate information about the government surveillance activity they are overseeing. Part III.B then goes on to address reforms aimed at the area most in need of attention—the court's rule-making performance—such as increasing the adversarial nature and transparency of the FISA Court's operations. It concludes that the legislative choices reflected in the USA FREEDOM Act fail to recognize just how inadequate FISA's procedures proved to be for a court expected to engage in rule making. As a result, the Act's reforms gesture in the right direction but fall far short of actually addressing the problem.

A. Reforms of the FISA Court's Gatekeeping Role

This Part first explains why the FISA Court's gatekeeping performance demonstrates that modifications to the makeup of the court are unnecessary and then considers the fact that, no matter how seriously the FISA judges take their oversight responsibilities, they can only be effective if they have the necessary information about the surveillance activities they have authorized. As neither the USA FREEDOM Act nor other proposals that have been floated go far enough in shoring up this aspect of FISA Court operations, I advance some suggestions with respect to how to do so.

1. Judicial Selection

The USA FREEDOM Act did well not to heed calls for modifying the makeup of the court and the means by which FISA judges are selected. Legislators, commentators, and even the President's Review Group have advocated several different ways to alter how FISA judges are chosen to serve on the court. At the heart of each of these proposals is an effort to redistribute the power over judicial selection. One proposal would include judges from each judicial circuit and require FISA Court of Review appointments to be approved by five Supreme Court justices.[205] Another would require FISA judges to be selected by the same process as Article III judges—appointment by the President with the advice and consent of the Senate.[206] Yet another would have FISA judges chosen as follows: three by the Chief Justice, two by the Speaker of the House of Representatives, two by the Senate

---

205. FISA Judicial Selection Reform Act of 2013, S. 1460, 113th Cong. (2013). The legislation would also have added two additional judges to the court. *Id.* § 3(a)(1)(B)(i).

206. Presidential Appointment of FISA Court Judges Act, H.R. 2761, 113th Cong. (2013).

Majority Leader, and two each by the House and Senate Minority Leaders.[207] Finally, the President's Review Group suggested that rather than lodging the appointment power in the Chief Justice alone, each member of the Supreme Court should have the authority to select one or two members of the court from within the circuit(s) over which they have jurisdiction.[208]

These proposals represent a solution in search of a problem. Most advocates for adjusting the court's selection process are motivated by the concern that the currently serving judges operate as rubber stamps. The accusation is that, because of their professional backgrounds or their political affiliations, FISA judges as currently selected are inclined to approve government surveillance applications without assessing them critically. To prove this allegation, critics point to the court's overwhelming rate of approval for government applications.[209]

High rates of approval, however, do not necessarily reflect a FISA Court bench partial to the government. First of all, the Justice Department lawyers responsible for preparing FISA applications know the standards that must be met and value maintaining their credibility before the court.[210] That the vast majority of applications are approved may be less about the judges' willingness to question the government than it is about government attorneys ensuring that their applications meet the necessary requirements. Second, FISA Court supporters note that the ninety-nine percent approval figure does "'not reflect the fact that many applications are altered prior to final submission or even withheld from final submission entirely, often after an indication that a judge would not approve them.'"[211] And finally, former FISA Judge James Carr attributes the government's success rate not to "spinelessness or excessive deference to the government" but instead to the forgiving standards that the government must meet.[212] Thus, the government's success rate may be more about the substance of surveillance law's requirements (or lack thereof) than it is about the FISA Court's application of that law.

Moreover, we have seen concrete examples of FISA judges operating with initiative and independence. We know that the FISA Court refused to authorize some section 215 applications "based on concerns that the investigation was premised on

---

207. FISA Court Accountability Act, H.R. 2586, 113th Cong. (2013).

208. PRESIDENT'S REVIEW GRP. REPORT, *supra* note 43, at 201, 208.

209. *See supra* Part I.B.

210. *See* Letter from Attorney Gen. Michael B. Mukasey to NYPD Comm'r Raymond W. Kelly (Oct. 31, 2008), *available at* http://online.wsj.com/public/resources/documents/WSJ_200811202Kelly.pdf [https://perma.cc/T435-CFJL]; *supra* text accompanying note 68.

211. PRESIDENT'S REVIEW GRP. REPORT, *supra* note 43, at 202 (quoting Letter from Hon. Reggie B. Walton, *supra* note 20). *But see* Donohue, *supra* note 76, at 831–32 (pointing out that only 2.6% of applications have been modified, only twenty-six have been withdrawn prior to FISA Court ruling, and out of 18,473 rulings, the FISA Court denied eight in whole and three in part). Without more information about the types of modifications that the Court has required and the bases on which applications have been rejected, it is impossible to determine the import of these numbers. *Id*. Evidence from the bulk collection context indicates, however, that the FISA Court takes its oversight role—at least in that context—very seriously. *See supra* Part II.A.

212. Carr, *supra* note 62.

protected First Amendment activity."[213] And recall Judge Kollar-Kotelly's treatment of the pen/trap provision that specified that "'the judge shall enter'" a surveillance order if the application includes each element listed in the statute, including a certification that the surveillance will likely obtain "'foreign intelligence information . . . or is relevant to an ongoing investigation to protect against international terrorism.'"[214] This statutory language plainly sought to limit judicial oversight of such applications to ensuring that the application included the relevant certification; it authorized no judicial assessment of the accuracy or validity of the statements contained in the certification. Yet in the face of this language, Judge Kollar-Kotelly insisted that FISA judges retained the power to look behind the assertions on government applications and evaluate not only whether they included all the required elements but also that those elements were accurate representations.[215] These are not the acts of a rubber stamp.

The other justification for modifying the FISA judge selection process is the President's Review Group's concerns about the lack of diversity among FISA judges. This proposal seems to assume that a more diverse slate of judges would include members more likely to push back against government applications. But while in the abstract greater diversity of judges—whether based on geography, ideology, or professional background—is a good thing, FISA judges have exhibited similar strengths and weaknesses. Whether appointed to the bench by Republican or Democratic presidents, they have excelled at gatekeeping (when they have adequate information) and have failed at rule making. Changing the makeup of the court itself, or how judges are selected to serve on it, will not address the FISA Court's true weaknesses; the USA FREEDOM Act's omission of provisions along these lines is thus entirely appropriate.

2. Ensuring the FISA Court is Fully Informed

Guaranteeing that the FISA Court has all of the information it needs to be an effective gatekeeper is one area of reform that has received insufficient attention. The court potentially suffers from lack of two types of information—information about how the executive branch is implementing the court's orders, and expertise in the highly technical aspects of surveillance operations. The former is critically important for the court to function as an effective gatekeeper. The latter is more central to effective rule making and will be discussed in Part III.B.

While the need for increased transparency of the court's operations has been front and center of FISA Court debate, the need to increase the flow of information to the court has been neglected. Even conceding that the FISA Court does not operate as a rubber stamp, lack of information about what the government is doing places a significant limitation on the FISA Court's ability to engage in effective oversight. When the court is aware of government noncompliance, FISA judges have been able to devise mechanisms to monitor, deter, and remedy it. But often this happened only

---

213. OFFICE OF THE INSPECTOR GEN., *supra* note 93, at 73; *see supra* note 93 and accompanying text.

214. Judge Kollar-Kotelly's Pen/Trap Opinion, *supra* note 54, at 25–26 (quoting 50 U.S.C. § 1842(c)(2), (d)(1)).

215. *See supra* notes 153–55 and accompanying text.

after years of ongoing government violations. And while the FISA Court has put to use its power to demand additional information from the government, that power is only effective for so-called "known unknowns." When it comes to compliance issues about which the court remains in the dark, the power to seek information is an empty letter. As is so often the case when it comes to oversight of classified government programs, the fundamental challenge here is that the FISA Court lacks the tools to independently verify how its orders are being carried out. We must therefore seek mechanisms designed to determine when (or how often) those orders are violated and to verify the government's characterizations of its own activities.[216]

a. Existing Information-Sharing Effectiveness

As the now-public FISA Court documents show, the government time and again belatedly informed the court of instances of noncompliance—noncompliance that had sometimes persisted for years and for which the NSA could offer no satisfactory explanation.[217] For a time, it seemed that close examination of any compliance problem simply revealed additional concerns.[218] And it was not until 2008 that the government alerted the FISA Court to the fact that ECPA might limit the NSA's power to disseminate information that had been collected under section 215 since 2006.[219]

---

216. *See* March 2, 2009, Order, *supra* note 100, at 12 ("[T]he Court must rely heavily on the government to monitor [any classified surveillance program] to ensure that it continues to be justified, in the view of those responsible for our national security, and that it is being implemented in a manner that protects the privacy interests of U.S. persons . . . ."); Carol D. Leonnig, *Court: Ability To Police U.S. Spying Program Limited*, WASH. POST, Aug. 15, 2013, https://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html [https://perma.cc/7B29-7AVJ].

217. *See* Oct. 3, 2011, Memorandum Opinion, *supra* note 122, at 16 n.14 (pointing out that there were at least three instances "in less than three years in which the government . . . disclosed a substantial misrepresentation regarding the scope of a major collection program"); Donohue, *supra* note 76, at 808 (citing Declaration of Lt. Gen. Alexander, *supra* note 104, at 27–28) ("Although the NSA had been contravening the order since May 2006 [regarding RAS for selectors], it was not until early 2009 . . . that the illegal behavior was brought to FISC's attention."). In addition to violations discussed in Part II, *supra*, DOJ informed the FISA Court of at least seventy-five additional instances in which it had provided false or misleading information in an application for a surveillance order, Philip Shenon, *Secret Court Says F.B.I. Aides Misled Judges in 75 Cases*, N.Y. TIMES, Aug. 23, 2002, http://www.nytimes.com/2002/08/23/us/secret-court-says-fbi-aides-misled-judges-in-75-cases.html [https://perma.cc/W7ZC-K8B8], and the NSA has conceded that it has engaged in significant overcollection under its FISA Amendments Act authority, *see* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633, 1655 (2010).

218. *E.g.*, March 2, 2009, Order, *supra* note 100, at 13 ("[T]he Court is very disturbed to learn that [the end-to-end review] has identified additional violations of the Court's orders, including . . . using telephone identifiers that had not been determined to meet the [RAS] standard.").

219. *See* Dec. 12, 2008, Supplemental Opinion, *supra* note 195, at 1–5.

Promoting the flow of this type of information to the court would allow the court to be a more proactive gatekeeper, amplifying its effectiveness and reducing the duration of noncompliance incidents. Some of the court's existing procedures aim to minimize the frequency of situations in which the court is left in the dark. Rule 13 of the FISA Court's procedures, for example, requires the government to alert the court to misstatements and instances of noncompliance.[220] And the NSA's creation of an Office of Compliance is also a step in the right direction. But as it stands, the court remains entirely dependent on the government informing it about the programs that it approves. On at least one occasion, a FISA judge declared that "the Court no longer [had] confidence" that the information it received from the government indicating that the NSA was complying with the court's orders was accurate.[221]

Existing rules and institutions, in other words, have not been sufficient to ensure that the FISA Court has the information it needs. And while the USA FREEDOM Act increased transparency requirements for the court's activities, it does little to increase the flow of information to the court.[222]

b. Comparing the FISA Court to Other Information-Sharing Challenges

The challenge of ensuring sufficient information flow from actors who benefit from not sharing information is not unique to the FISA Court context. Consider three information holders who might resist disclosing full and accurate information: prosecutors obligated to disclose to the defendant exculpatory information pursuant to *Brady v. Maryland*,[223] law enforcement officials testifying regarding circumstances surrounding a search or seizure that has been challenged as unconstitutional, and intelligence officials required to keep congressional intelligence committees "fully and currently informed" about ongoing surveillance activities.[224] In each of these areas, the entity in possession of relevant information can benefit from keeping that information secret—prosecutors are more likely to win convictions if defendants lack exculpatory information, law enforcement officials avoid exclusion of evidence they discovered if a judge is unaware that the evidence was gathered in violation of the Fourth Amendment, and intelligence agencies retain more autonomy and flexibility when overseers lack knowledge of their activities. Government actors' failure to fulfill their disclosure responsibilities in these contexts has proved resistant to reform. Consequently, skepticism regarding whether the situation can be improved in the FISA Court context is to be expected. There are good reasons to believe, however, that the kinds of reforms that have had only modest impact elsewhere are more likely to prove effective in assisting the FISA Court in acquiring necessary information.

---

220. FISA CT. R. 13.

221. March 2, 2009, Order, *supra* note 100, at 12.

222. *See infra*, Part III.B. (discussing the USA FREEDOM Act's transparency measures).

223. 373 U.S. 83, 87 (1963) (holding that due process requires prosecutors to disclose to the defense materially exculpatory evidence, including evidence that goes toward negating a defendant's guilt, that would reduce a defendant's potential sentence, or evidence going to the credibility of a witness).

224. 50 U.S.C.A. § 3092(a)(1) (2015) (formerly codified at 50 U.S.C. § 413a).

A brief discussion of other information-flow challenges and ideas for their reform will highlight the ways in which the FISA Court is more amenable to reform. First, consider the context of prosecutors' disclosure obligations under *Brady*. As commentators have pointed out for years, a prosecutor's desire to gain convictions frequently results in a failure to provide the defense with all the relevant exculpatory information. Professor Miriam Baer has canvassed the many reform proposals seeking to minimize such violations and grouped them into three categories.[225] The first category expands the scope of materials that the prosecutor must disclose.[226] This type of reform is premised on the idea that prosecutors alone cannot effectively provide to the defendant the information to which he is entitled. Another set of eyes—eyes looking through a lens not focused on attaining a conviction—is required.[227]

The second type of *Brady* reform is to boost "the likelihood and degree of sanctions for noncompliance."[228] Under current law, prosecutors who violate *Brady* are immune from civil liability, and their supervisors are immune from claims founded on allegations of poor oversight or poor training.[229] Prosecutors can themselves be prosecuted criminally, be held in contempt, or be subjected to professional sanctions by their state bar officials, but critics point to the infrequency with which these sanctions are employed.[230] This situation has prompted some reformers to propose that courts make more use of a wider range of sanctions, including some that are less draconian, speculating that sanctions are more likely to be imposed if there are options short of criminal or contempt charges.[231]

The third category of proposed *Brady* reforms involves efforts to improve "the internal processes and organizational dynamics of the offices in which prosecutors work."[232] Such improvements include additional training, efforts to modify social norms, internal compliance programs, and the like.[233] Former Attorney General Eric Holder championed this type of approach when, among other reforms, he created a "national discovery coordinator," "required each U.S. Attorney's Office to designate a *Brady* coordinator[,] and required each office to verify that it had trained its attorneys in *Brady* and its progeny."[234] Lodging responsibility for institutional *Brady* compliance with specific individuals arguably places pressure on those individuals to ensure their colleagues follow the rules.

---

225. Miriam H. Baer, *Timing* Brady, 115 COLUM. L. REV. 1, 22–31 (2015).

226. *Id.* at 5 (providing as an example what is known as an "open-file regime," in which the prosecutor makes all relevant evidence available, and the defendant decides what to consider exculpatory (internal quotation marks omitted)).

227. *Id.* at 24–25.

228. *Id.* at 26.

229. *Id.*

230. *Id.* at 28 ("Even in recent years, only in the most egregious cases have prosecutors been publicly criticized, censured, or disbarred, leading some scholars to conclude that *Brady*'s primary enforcement mechanism is little more than a 'paper tiger.'" (italics in original)).

231. *Id.* at 27–28.

232. *Id.* at 22.

233. *Id.* at 28–29.

234. *Id.* at 30 (italics in original).

The phenomenon of law enforcement officials providing false testimony regarding their investigative actions is another area that presents information-flow challenges, and it is so common that it has its own name—"testilying." Like *Brady* violations, the offense occurs regularly[235] and is rarely sanctioned.[236]

Many suggestions for reform have been made in this context as well. Professor Christopher Slobogin argues that the exclusionary rule creates such strong incentives to lie that the only way to reduce "testilying" is to abandon the exclusionary rule itself. If truthful testimony about arguably unconstitutional acts would not result in suppression of evidence, officers might feel less pressure to prevaricate. Instead, he suggests imposing severe punishments for perjury, rewards for providing testimony that is corroborated by other evidence, and a damages remedy for victims of unconstitutional law enforcement activity.[237] Others have similarly suggested a focus on replacing evidence suppression with disciplinary action against offending officers. Penalties could be extreme—such as dismissal from the force—or more moderate—fines, loss of vacation time, official reprimands, etc.[238]

In both of these contexts, serious concerns about the thoroughness of information sharing has arisen, and in both of them reform proposals have fallen into similar categories. First, they suggest modifying the operative rule to reduce perverse incentives—whether by making sure that the prosecutor is not the only one to see the information in her possession, or by eliminating the exclusionary rule. Second, they call for a wider spectrum of available sanctions for improper nondisclosure, recognizing reluctance to impose criminal or career-ending sanctions against law enforcement officials. Finally, they all envision a role for organizational reforms—such as increased training and modification of reporting or responsibility structures.

While these reforms have had a limited effect on *Brady* violations and "testilying," applying them to the FISA Court should prove much more effective. First, consider the differences in incentive structure. Taking NSA officials at their word, failure to report information to the FISA Court has been unintentional. Unlike misbehaving prosecutors or perjuring police officers, the NSA did not fail to disclose information it knew to be relevant to the lawfulness of its actions; it simply failed to recognize that it had such information. And, once it was discovered, the agency

---

235. I. Bennett Capers, *Crime, Legitimacy, and Testilying*, 83 IND. L.J. 835, 870 (2008) (citing studies indicating that instances of police perjury are "so pervasive that even former prosecutors have described them as 'commonplace' and 'prevalent'" (footnotes omitted)); *id.* at 871 (an investigation into the NYPD "found evidence of police supervisors instructing their officers how to lie so that evidence obtained in violation of the Constitution would not be suppressed"); Christopher Slobogin, *Testilying: Police Perjury and What To Do About It*, 67 U. COLO. L. REV. 1037, 1045–48 (1996); Myron W. Orfield, Jr., Comment, *The Exclusionary Rule and Deterrence: An Empirical Study of Chicago Narcotics Officers*, 54 U. CHI. L. REV. 1016, 1049–50 (1987) (Seventy-six percent of responding police officers agreed that police officers shade the facts to establish probable cause).

236. Capers, *supra* note 236, at 871–72 ("[E]xamples of supervisors expressing their unwillingness to investigate and discipline officers abound.").

237. Slobogin, *supra* note 236, at 1055–59; *see also* Capers, *supra* note 236, at 871–75 (advocating, as an alternative remedy, increased frequency of prosecution for "testilying").

238. *See* Capers, *supra* note 236, at 871 (quoting Hon. John F. Keenan, *The Proper Balance: Exclusion of Evidence or Expulsion of Police Officers*, 72 ST. JOHN'S L. REV. 1376, 1380 (1998)).

promptly informed the court. This means that the problem to date has not been so much that the NSA has overwhelming incentives to withhold information that it has but instead that it failed to recognize that it even had such information.

Moreover, even assuming that (at least some) NSA noncompliance has been intentional, any benefit that flows from withholding information is much more intangible in the FISA context. When police find incriminating evidence, or prosecutors find exculpatory evidence, the value of that information for the prosecution or the defense, respectively, is clear. The more critical the evidence, the greater the incentive to ensure that it is admissible (in the case of police discovery of incriminating evidence) or not provided to the defendant (in the case of a prosecutor with exculpatory evidence). Prosecutors and police officers who admit noncompliance are thus faced with the possibility that a specific alleged criminal—one whose crime they have invested time and energy in investigating and preparing to prosecute—will go free, adversely affecting both the public safety and possibly the individual officer's or prosecutor's own career prospects. If the NSA fails to comply with the rules, by contrast, the result might be destruction of the information and any work product based on that information—with uncertain and difficult to define consequences—or additional controls on information's collection and use. There is no specific, tangible result; the world is no worse off than it was before the violation (though there may be career implications for the official). The uncertain value of the information means that the incentives to retain it or to continue collecting information like it are not as strong. This means that effective solutions in the FISA Court context need not involve drastic modifications to the existing incentives to counteract the overwhelming pressure to withhold information that actors in the criminal justice system face.

Second, consider the impact of these differences on the imposition of sanctions. Sanctions against prosecutors and police officers are relatively extreme—prosecution, loss of law license, contempt sanctions—and judges have proved reluctant to impose them. Recognizing that most noncompliance is inadvertent, sanctions would constitute charges of carelessness, not maliciousness. They would therefore not carry the moral approbation that accompanies charges of prosecutorial misconduct or perjury. Judges' and supervisors' decisions to impose sanctions would therefore be less fraught, especially if the sanctions represented a wide range of possibilities as reformers in other areas have suggested.

Third, because the information withheld from the FISA Court is hoarded inadvertently as opposed to intentionally, remedies aimed at assisting the NSA itself to uncover misconduct could be effective in a way that they have not been in the criminal context. Thus, internal institutional controls aimed at uncovering relevant information could prove particularly effective when it comes to FISA. If the challenge is to discover problems, as opposed to convincing the agency to reveal noncompliance, then modification of internal processes could yield benefits that have eluded prosecutors' offices.

Yet another information-sharing challenge is perhaps the most analogous to what the FISA Court faces: Congress's efforts to remain sufficiently informed about secret government activities. The President is statutorily obligated to ensure that the congressional intelligence committees are kept "fully and currently informed" of U.S. intelligence activities, as well as "significant anticipated intelligence

activity."[239] This is usually accomplished through periodic briefings from the intelligence community officials to the chairs and ranking members of the House and Senate intelligence committees, who then (usually) make that information available to the rest of the committee. As with the FISA Court, this mechanism makes it difficult to uncover "unknown unknowns"—Congress can only ask questions about things of which it is aware—and throughout the intelligence committees' history, there has been great debate with respect to whether this system is effective.[240]

The FISA Court should be able to engage in more effective oversight than Congress. To be sure, Congress's entitlement to information is statutorily mandated, and Congress possesses several tools with which it can pressure the executive branch for information should it want to do so.[241] But even if Congress wanted to use its levers of power to engage in aggressive oversight, it is like the FISA Court in that it has no mechanism for determining when it is getting the full story, and when it should be digging for "unknown unknowns"—even aggressive oversight requires legislators to know what questions they should be asking.[242] Moreover, as I have argued elsewhere, legislators' incentives press against aggressive intelligence oversight.[243] And as Edward Snowden's leaks have amply demonstrated—legislators knew about the section 215 metadata program since its inception—even the information that Congress does have may not be shared publicly, thereby significantly limiting its power to impact oversight.

The FISA Court does not share these institutional deficiencies when it comes to oversight. As an initial matter, FISA judges need not seek reelection, so the political dynamics that limit legislators do not present an obstacle to FISA judges. Perhaps more importantly, however, FISA judges are much better positioned to discover the "unknown unknowns" that may exist. Whereas Congress gets a birds-eye view of the surveillance apparatus from intelligence officials' briefings, FISA judges are involved with the day-to-day implementation of the various FISA-authorized surveillance programs. Judges thus have much more detailed information about the programs they are overseeing, receive more frequent updates with respect to the implementation of those programs, and generally are much more knowledgeable than Congress about the details and the mechanics of the surveillance programs they authorize. This means they are more likely to see red flags than legislators. They are also in a position to require the government to provide detailed, targeted reporting designed to explore red flags and ferret out compliance problems.

---

239. 50 U.S.C.A. § 3091(a)(1) (2015).

240. *See* Emily Berman, *The Paradox of Counterterrorism Sunset Provisions*, 81 FORDHAM L. REV. 1777, 1811–13 (2013) (discussing deficiencies of congressional oversight of intelligence activities).

241. If Congress wants to pressure the executive branch to be more forthcoming with information, it may employ the power of the purse to limit executive appropriations, initiate investigations into executive branch activity, hold hearings to publicize issues that it wants to spotlight, etc.

242. *See* Berman, *supra* note 241, at 1811.

243. *Id.* at 1818–20.

c. Information-Sharing Reforms

This comparative institutional analysis helps determine both the likely value of existing FISA Court procedures as well as what sort of additional steps should be taken. As for existing measures, some have come from the NSA itself. In the wake of the major compliance problems revealed in 2009, the NSA made some changes. Recognizing that "its compliance and oversight infrastructure had not kept pace with its operational momentum and the evolving and challenging technological environment in which it functioned," the NSA sought to "address these issues from a structural and managerial perspective, including thorough enhancements to its compliance structure."[244] The result was the creation of the position of the Director of Compliance, "whose sole function is to keep all of NSA's mission activities consistent with the law and applicable policies and procedures" as well as "regular detailed senior leadership reviews of the compliance program."[245] The NSA has also enhanced its oversight coordination with the Office of the Director of National Intelligence (ODNI) and the Department of Justice (DOJ).[246]

These measures implement ideas similar to those floated in the criminal context to improve management and concentrate compliance responsibility in one institution, such as the creation of a national discovery coordinator. And to the extent that entities outside the NSA are involved—such as the ODNI or DOJ—they also mirror the category of *Brady* reforms that rely on having an independent set of eyes review relevant material. The suggested reform they have not adopted—at least explicitly—is the creation of a system of rewards and sanctions aimed at full information disclosure.

Exploiting their intimate knowledge of the NSA's operations, FISA judges themselves have implemented some additional measures. Many of these are also structural and management-related modifications designed to uncover the inadvertent nondisclosure that has been so problematic for the NSA, and they represent the kind of detailed micromanagement that congressional overseers cannot match. Examples include mandatory spot checks, required involvement from the Justice Department's National Security Division—the mechanism through which at least one major compliance problem was identified[247]—and periodic reports to the FISA Court regarding the collection and dissemination of metadata and metadata-derived information. The USA FREEDOM Act supports FISA judges' authority to impose such requirements in section 401 where it specifies that the Act's authorization for the court to appoint an amicus curiae under certain circumstances is not meant to "limit the ability of [the court] to request or receive information" from

244. Press Release at 2, James R. Clapper, Dir. of Nat'l Intelligence, DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA) (Sept. 10, 2013), *available at* https://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document.

245. *Id.*

246. *Id.*

247. *See supra* notes 129–32 and accompanying text.

the government.[248] The Court should continue to employ these mechanisms aggressively to identify early any compliance problems that arise.

But more can, and should, be done. The PCLOB has endorsed at least one promising measure in the context of the section 702 program. In addition to any audits or reports that the NSA must submit to Congress, the PCLOB suggests that, "the government should submit with [its section 702 program applications] a random sample of [its collection results] and a random sample of the [query terms], with supporting documentation."[249] This in effect permits the court to perform its own spot check of the government's activities, bringing an additional, unbiased set of eyes to the material. Similar requirements could be imposed on any collection program, and the FISA Court could use this information to verify that the government's representations about its activities during the previous certification period were accurate.[250]

In addition, existing compliance mechanisms must come attached with consequences and rewards. Just because a particular instance of noncompliance is inadvertent does not mean that nobody should be held responsible. As Judge Walton pointed out, many of the NSA's systemic compliance problems stemmed from the fact that nobody had a sufficiently comprehensive understanding of the programs being implemented. One solution to this type of problem is to implement measures, like spot checks, that in effect force supervisors and high-ranking officials to pay more attention. But that solution is likely to be even more effective if supervisors are sanctioned for failing to discover noncompliance that they reasonably should have prevented or discovered earlier. To the extent previous issues arose from simply turning a blind eye to possible concerns, sanctions would improve compliance.

FISA judges or NSA supervisors could be empowered to impose a broad menu of sanctions on officials who fail to take reasonable measures to prevent, deter, and detect overcollection. These sanctions could range from dismissal, to loss of vacation time, to an official reprimand, to loss of security clearance. This is not to say that NSA officials should not be subject to much more stringent penalties—up to and including criminal charges—for noncompliance that rises to that level. But it does recognize that most noncompliance does not fit that description, and aims to create a sanctions regime tailored to the level of culpability—incompetence, negligence, or lack of technical understanding—that is usually on display. Sanctions should be accompanied by positive reinforcement. Just as Professor Slobogin proposes rewards for police officers that present corroboration for their testimony,[251] NSA officials who are particularly diligent in preventing or detecting overcollection should be rewarded. Rewards could be concrete—financial bonuses or extra vacation time, for example—or less tangible—an award or commendation.

In sum, judges and legislators should pay more attention to ensuring the FISA Court has the information it needs to be an effective gatekeeper. And while some

---

248. USA FREEDOM Act of 2015, Pub. L. No. 114-23, sec. 401, § 103(i)(10), 129 Stat. 268, 279–80 (to be codified at 50 U.S.C. § 1803).

249. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 141 (2014) (italics omitted) [hereinafter PCLOB SECTION 702 REPORT].

250. *Id*.

251. *See supra* text accompanying note 238.

measures already are in place, we know from other contexts where information sharing is a challenge that there are additional ways to improve the situation.

B. Reforms of the FISA Court's Rulemaking Role

In Part II.B, I argued that the primary flaw in the court's performance has been its failure to address, or to engage fully with, possible counterarguments to the government's position when serving in its rulemaking role.[252] This flaw stems from the fact that the court was designed as a gatekeeper, and several structural features of that regime are ill-suited to rule making. As a result, those features as they existed before the enactment of the USA FREEDOM Act have been the subject of widespread critique.[253] First, the FISA Court's essentially nonadversarial nature meant that FISA judges were not provided with counterarguments or critiques of the government's position. Second, there was no institutionalized means of challenging a FISA judge's initial analysis. While most Article III courts are constrained by the prospect of appellate review and the requirement that they provide a public, reasoned explanation for their decisions, FISA judges have operated on the (usually accurate) assumption that their opinions will be the final word on the issue and that they will remain secret. Which leads to the third concern—lack of transparency. Finally, the court must be able to understand the technical nuances of the programs whose lawfulness it interprets. As such, FISA judges must have access to sufficient technical expertise. The USA FREEDOM Act purportedly targets each of these flaws, but the result is a mere tinkering around the edges of the existing structure, rather than the significant modifications necessary to implement meaningful change.[254]

1. Adversarial Proceedings

Nearly all FISA Court reform proposals have recognized that if the court is to continue to operate as rule maker for programs permitting nonindividualized surveillance, its proceedings must incorporate adversarial elements.[255] The

252. *See supra* Part II.B.

253. *See supra* Part I.B.

254. Measures that will improve the court's lawmaking performance would not impair, and in some cases might aid, the court's gatekeeping performance as well. Given the court's performance, however, these measures are much more important in the context of the court's law-making role than they are in the gatekeeper context.

255. *E.g.*, FISA Court Reform Act of 2013, S. 1467, 113th Cong. § 3 (2013); ACLU v. Clapper, 785 F.3d 787, 829–31 (2d Cir. 2015) (Sack, J., concurring); Remarks on United States Signals Intelligence, *supra* note 35, at 5; PCLOB SECTION 215 REPORT, *supra* note 34, at 183 ("Congress should enact legislation enabling the FISC to hear independent views . . . on novel and significant applications . . . ." (italics omitted)); PCLOB WORKSHOP, *supra* note 42, at 36–37 (statement of Hon. James Robertson, former FISA Court judge); PRESIDENT'S REVIEW GRP. REPORT, *supra* note 43, at 200–05; Margulies, *supra* note 59, at 52–62; Letter from the Liberty and Sec. Comm. of the Constitution Project to Members of Congress (May 20, 2014), *available at* http://www.constitutionproject.org/wp-content/uploads/2014/05/TCP-Letter-to-House-members-on-FISA-Special-Advocate.pdf [https://perma.cc/48ED-26YN] [hereinafter Constitution Project Letter]. *But see* GOITEIN & PATEL, *supra* note 21, at 45 (arguing that the

adversarial process is what the American judicial system relies upon to ensure that novel legal arguments are vetted thoroughly. It is premised on the idea that only by hearing from both parties, each with a concrete stake in the outcome, will the court be presented with the strongest arguments on each side.[256] Indeed, when a case raises relevant arguments that are not supported by any of the parties to the litigation, federal courts will sometimes appoint amici to present those arguments in the most comprehensive, persuasive way.[257] And while adversarial proceedings are not a panacea—courts reach controversial or inaccurate conclusions all the time—the odds of reaching the best results improve when courts have all arguments in front of them.

It follows that when the court is engaged in rule making, its assessment of the government's position is much more likely to avoid oversights or errors, and the quality of the FISA Court's analysis and decision making will improve if there is a party tasked with presenting the best case against the government's position. An adversarial system would also force the court to weigh these arguments and explain why it selected one side over the other.[258] Improvement in this regard will produce not only higher quality opinions and analysis, but also provide additional credibility. If the government's bulk-collection activities are approved by a FISA Court that thoroughly vetted the best arguments on each side, the validity of that determination will be more difficult to challenge.

In the context of section 215, there is reason to believe that adversarial proceedings would have yielded a very different result. Prior to the Snowden leaks, section 215's bulk-collection program was renewed over thirty times by over a dozen different FISA Court judges. None of these judges rejected the government's position and none wrote an opinion examining the lawfulness of the program. After the leaks, two FISA Court decisions upheld the program, but a traditional federal district court

---

FISA Court should never interpret novel questions and therefore does not require adversarial proceedings); Donohue, *supra* note 76, at 806–24 (arguing that rule making is beyond the scope of what Congress envisioned for the FISA Court); Kerr, *supra* note 30, at 1532–43 (arguing that the FISA Court should not have adversarial proceedings because it should not be hearing and deciding novel questions); Letter from Hon. Alex Kozinski, Chief Judge, Ninth Circuit Court of Appeals, to Hon. Patrick J. Leahy, Chairman, Senate Comm. on the Judiciary (Aug. 14, 2014), *available at* http://images.politico.com/global/2014/08/20/kozinski_to_leahy.html [https://perma.cc/5VZV-HWY3] (noting that he has "serious doubts" about Judge Bates' views).

256. *See Clapper*, 785 F.3d at 829–31 (Sack, J., concurring) (describing how the adversarial system swayed the district court judge's opinion in the landmark "Pentagon Papers" case); PCLOB WORKSHOP, *supra* note 42, at 34 (Hon. James Robertson stating, "[I]t's the norm to read one side's brief or hear one side's argument and think, hmm, that sounds right, until we read the other side."); Carr, *supra* note 62 (a former FISA Court judge pointing out that during his six years on the FISA Court, "there were several occasions when I and other judges faced issues none of us had encountered before. A staff of experienced lawyers assists the court, but their help was not always enough given the complexity of the issues.").

257. *See, e.g.*, Alderman v. United States, 394 U.S. 165, 183–84 (1969) (noting that adversarial proceedings become more important the more complex the question with which the court is confronted); Brief for Court-Appointed *Amica Curiae* Addressing Jurisdiction, United States v. Windsor, 133 S. Ct. 2675 (2013) (No. 12-307) (addressing arguments challenging the Court's jurisdiction over the case).

258. Margulies, *supra* note 59, at 52–53.

and a federal circuit court—with the benefit of the adversarial process—came out the other way.[259] Moreover, the majority of the PCLOB, which had the benefit of extensive input from experts on all sides of the issue, concluded that the program was not authorized by statute.[260]

Nearly every proposal to reform FISA Court operations agreed that an adverse party should participate in at least some FISA Court proceedings to inject adversarial process. "Whether called a 'special,' 'public,' 'public interest,' or 'constitutional' advocate, the core idea is the same—that a security-cleared lawyer should have the opportunity to challenge the government's factual and legal case before the [FISA Court]."[261] The proposals varied, however, with respect to where such an entity would be housed, from what pool of individuals or institutions it would be drawn, who would select it, and what powers it would have.[262] Other variations include what cases that entity would participate in, what interests it would represent, to what information it would have access, and whether it could initiate an appeal or declassification of a FISA Court decision.

The original—and most robust—form of the idea would have created an "Office of the Special Advocate" within the judicial branch.[263] The Special Advocate would be chosen by the Chief Justice for a renewable three-year term, and could only be removed for cause. In addition to arguing in support of legal interpretations that protect individual privacy and civil liberties, the Special Advocate would have access to any documents or other materials necessary, could move the court to reconsider any decision, and could petition for a decision (or a summary of a decision, if it included classified information) to be disclosed publicly. Review of any decision appealed by the Special Advocate would be essentially mandatory, and the Special Advocate could appeal adverse decisions of the FISA Court of Review to the Supreme Court. Critically, the Special Advocate herself would determine when to seek to participate in FISA Court proceedings.[264]

---

259. *See Clapper*, 785 F.3d at 821 (holding that the telephony metadata program was not consistent with the statutory language in section 215); Klayman v. Obama, 957 F. Supp. 2d. 1, 41 (D.D.C. 2013) (holding that the plaintiffs were likely to succeed on their claim that the section 215 program violated the Fourth Amendment), *vacated and remanded on other grounds*, 800 F.3d 559 (D.C. Cir. 2015).

260. *See supra* note 167 and accompanying text.

261. Stephen I. Vladeck, *The Case for a FISA "Special Advocate,"* at 7 (Jan. 7, 2015) (unpublished manuscript, on file with the *Indiana Law Journal*).

262. *See, e.g.*, USA FREEDOM Act, H.R. 3361, 113th Cong. § 401 (2014); FISA Court Reform Act of 2013, S. 1467, 113th Cong. § 3 (2013); Ensuring Adversarial Process in the FISA Court Act, H.R. 3159, 113th Cong. § 2(b)(5) (2013); FISA Improvements Act of 2013, S. 1631, 113th Cong. § 4 (2013); Remarks on United States Signals Intelligence, *supra* note 35; GOITEIN & PATEL, *supra* note 21, at 45–46; PRESIDENT'S REVIEW GRP. REPORT, *supra* note 43, at 203–05; Carr, *supra* note 62; Braun, *supra* note 42; Constitution Project Letter, *supra* note 256; *see also* Vladeck, *supra* note 262 (describing in detail the various proposals for a FISA advocate and their differences).

263. This description of the proposed Office of the Special Advocate relies upon Vladeck, *supra* note 262.

264. *See* Vladeck, *supra* note 262, at 7–8 (describing the initial vision for the role of the Special Advocate).

There was significant resistance within the intelligence community, however, to creating a truly independent Special Advocate, and the original proposal was diluted.[265] Ultimately, the version of the Act that was enacted embraces the idea of encouraging FISA judges to appoint amici rather than creating a truly independent advocate. Under the USA FREEDOM Act of 2015, the FISA Court

> shall appoint an . . . amicus curiae to assist such court in the consideration of any application . . . that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate.[266]

Any amicus appointed pursuant to this section will provide the court with legal arguments that "advance the protection of individual privacy and civil liberties," "information related to intelligence collection or communications technology," or any other relevant arguments or information.[267] The court is also permitted to appoint an amicus to provide technical expertise or to approve a motion by an individual or organization to file an amicus brief.[268] As a result, the legislation includes some adversarial elements.

Unfortunately, these new adversarial elements will produce only a negligible effect. The first problem with the Act's amicus provision is that it leaves the ultimate determination of when an adverse party participates to the court. In addition to the fact that the FISA Court—like any federal court—already possesses the power to appoint amici, part of the value of creating an adversarial process is in having a counterparty that may see arguments or issues that the FISA judges and the government do not recognize. The strength of the adversarial process comes not from the power of the courts to seek input when they so desire, but from a guarantee that each side will be presented in its most convincing form. It should therefore not be for the FISA Court to decide whether an opposing party might have something to add. Instead, it should be an advocate's job to determine when a government application raises a privacy or civil liberty concern to which it wants to respond. The power to determine when to intervene should rest with the advocate, not the court.[269]

Indeed, we have already seen indications that the amicus model falls short. In his opinion and order of June 17, 2015, Judge F. Dennis Saylor IV considered the question whether the USA FREEDOM Act, which was enacted after section 215 had been allowed to expire, reinstated the relevant expired provisions and amended them, or amended the version of the law to which section 215 reverted when it expired on

---

265. *See id*. at 13 (noting that a version of the USA FREEDOM Act that did not include an independent special advocate was the result of "a series of hard-fought compromises" among stakeholders, including *inter alia*, the intelligence community).

266. USA FREEDOM Act of 2015, Pub. L. No. 114-23, sec. 401, § 103(i)(2)(A), 129 Stat. 268, 279 (to be codified at 50 U.S.C. § 1803).

267. *Id*. sec. 401, § 103(i)(4).

268. *Id*. sec. 401, § 103(i)(2)(B).

269. I would argue that any matter involving approval of nonindividualized surveillance should be subject to adversarial proceedings. But there may be other types of cases for which an advocate's participation is appropriate. I would therefore not limit the advocate's participation to cases of rule making.

midnight on May 31, 2015. As Judge Saylor conceded, the question undoubtedly presents a "significant" legal issue and may present a "novel" one as well.[270] Under the USA FREEDOM Act, FISA judges "shall appoint" an amicus to assist when considering "novel or significant" legal issues "unless the court issues a finding that such appointment is not appropriate."[271] Here, Judge Saylor found the appointment of an amicus not appropriate "because the legal question is relatively simple, or is capable of only a single reasonable or rational outcome."[272] Determining that "no reasonable jurist would reach a different decision" than he, no amicus needed to be appointed.[273]

This application of amicus provision undermines its very purpose. The entire premise behind the need for adversarial proceedings is that there are arguments that may seem, based on government submissions, to be obviously correct, but that when scrutinized by someone charged with considering alternative interpretations become less plainly wrong. In other words, the point is to ensure that, when faced with a significant or novel legal issue, the FISA judge will have the benefit of arguments on both sides of the question. A unilateral conclusion that reasonable jurists necessarily would decide the issue only one way is the very one-sided decision making that the amicus provision was meant to prevent.

This is not to say that Judge Saylor's conclusion that the USA FREEDOM Act reinstated and amended the pre-sunset version of section 215 is implausible. It is not, however, the slam dunk that Saylor portrays it to be. Indeed, a purely textual reading of the USA FREEDOM Act demands the opposite conclusion. The version of section 215 enacted in the PATRIOT Act very clearly ceased to be operable law at midnight on May 31, 2015.[274] So when the USA FREEDOM Act was passed and signed into law on June 2, 2015, the law already had reverted to its pre-PATRIOT Act form. The USA FREEDOM Act says nothing about reinstating a different version of section 215 or retroactively extending its sunset beyond June 1, 2015. Any conclusion that it did so requires a judge to look behind the language of the statute for extratextual evidence of a contrary congressional intent. Presumably these are the types of arguments that an amicus would have raised.

Moreover, Saylor ignores additional benefits that an amicus's involvement would yield. Even if Saylor's legal conclusion is correct, there is value in having novel questions resolved with the benefit of an adversary, because that will lead to higher- quality opinions, more well-thought-out arguments, and, consequently, added public legitimacy. Indeed, Saylor recognizes that an amicus "might help to develop and refine arguments and to clarify the reasoning of the court."[275]

---

270. Memorandum Opinion at 5, *In re* Applications of the Federal Bureau of Investigation for Orders Requiring the Production of Tangible Things, Nos. BR 15-77, 15-78 (FISA Ct. June 17, 2015) [hereinafter June 17, 2015, Memorandum Opinion] (internal quotation marks omitted).

271. Sec. 401, § 103(i)(2)(A), 129 Stat. 279.

272. June 17, 2015, Memorandum Opinion, *supra* note 271, at 5.

273. *Id.* at 6.

274. PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, sec. 2, 125 Stat. 216, 216 (extending the sunset for section 2015 to June 1, 2015).

275. *Id.* at 6 n.8.

Nevertheless, he eschews use of the mechanism here, and posits that in cases where amici would "result in some degree of additional expense and delay," they should not be employed.[276] Such considerations cannot be what Congress had in mind when permitting the FISA Court to decline to appoint an amicus when it was not "appropriate."[277] Employing an amicus in the FISA Court process will always result in some degree of additional expense and delay. It will use additional judicial resources. A briefing schedule that permits responses and replies will extend the time between a government filing and a final order. It will require additional hours from government lawyers and possibly even payment to compensate amici. So if it is not appropriate to use an amicus when it will result in any additional delay and expense, it is never appropriate to use an amicus. But Congress's determination in passing the USA FREEDOM Act was that the tradeoff here—some additional time and expense in return for a more effective, accurate legal process—was worthwhile. That decision is not the FISA Court judges' to make. It is a legislative judgment embedded in the law they must apply. The ineffectiveness of the amicus provision in the first time a FISA judge was faced with the obligation to appoint one demonstrates that when it comes to adding adversarial procedure, the USA FREEDOM Act falls short of what is required.

2. Appeals

Another critical reform to any process through which the FISA Court engages in rule making is providing the means to pursue appeals of progovernment decisions. Appeals, an inherent feature of an adversarial system, play a crucial role in any judicial rule making power. When novel questions of law are presented to a court, we do not necessarily expect them to be resolved perfectly the first time a court takes them under consideration. Rather, appeals courts review lower courts' reasoning due to the fact that "[c]ourts of appeals . . . are structurally suited to the collaborative juridical process that promotes decisional accuracy."[278] In the words of Justice Frankfurter, "that fruitful interchange of minds which is indispensable to thoughtful, unhurried decision and its formulation in learned and impressive opinions" can come only with "discussion," "reflection," and "study."[279] In other words, the most effective analysis of questions of law is a collaborative one, necessarily involving multiple judges. And while a single FISA judge is of course capable of great reflection and study, discussion—and the collaborative process it reflects—can come only with a panel of judges. Moreover, the prospect of judicial review "should encourage a district court to explicate with care the basis for its legal conclusions."[280]

---

276. *Id.* at 5 n.7.

277. Sec. 401, § 103 (i)(2)(A), 129 Stat. 279; *see* Elizabeth Goitein, *The FISC's Newest Opinion: Proof of the Need for an Amicus*, JUST SECURITY (June 23, 2015, 9:43 AM), https://www.justsecurity.org/24134/fiscs-newest-opinion-proof-amicus/ [https://perma.cc/MTU4-H3LE].

278. Salve Regina Coll. v. Russell, 499 U.S. 225, 232 (1991).

279. *Id.* (quoting Dick v. N.Y. Life Ins. Co., 359 U.S. 437, 458–59 (1959) (Frankfurter, J., dissenting)).

280. *Id.* at 233.

Thus the very availability of appellate review should improve the quality of the initial judges' opinions.

Prior to the passage of the USA FREEDOM Act, only the government had the power to appeal most FISA Court decisions; thus, those decisions were rarely subject to this collaborative review process. Novel and complex legal questions have therefore been left in the hands of the one man or woman who happened to be on duty the week that they arose. This system compounded the FISA Court's failure to fully analyze the government's justification for the bulk-collection programs by providing that one FISA judge's decision was in essence the final word on the subject.

The government is fond of defending the telephony metadata bulk collection program with the argument that fifteen federal judges have approved it. But what is likely a more accurate description is that one judge approved it, and fourteen others (as well as Congress) declined to challenge their colleague's conclusion. Moreover, as FISA Court orders addressing novel questions serve as persuasive authority in subsequent cases, one could argue that no judge considered the definition of "relevance" in the bulk telephony context. Rather, the first FISA judge faced with a section 215 application for bulk collection of telephony data simply relied upon Judge Kollar-Kotelly's interpretation of "relevance" in the pen/trap context, and all subsequent judges faced with the question (as well as Congress) accepted that interpretation.[281]

Moreover, existing debates ignore the fact that the errors emerging from the FISA Court appeals system will not occur at random. Assuming that appeals courts will not reach the proper result 100 percent of the time, FISA's asymmetrical appeals structure, which permits only the government to appeal adverse decisions, has predictable effects on both the outcome of cases and the development of the substantive law. As an initial matter, permitting only the government to appeal means that any erroneous judgments are more likely to be "wrong" in the government's favor—in other words, the FISA Court and FISA Court of Review are more likely to approve surveillance requests that should have been denied than to deny requests that should have been granted.[282] This is an intuitive result. For any application that should be denied, the government has two opportunities to convince a court that it should be approved. First, there is the FISA judge. As no decision maker is perfect, the FISA Court will at times grant orders it should deny—in other words, the FISA judge will sometimes issue false positives—and there is no means to subject that (incorrect) decision to appellate review. If the FISA judge does deny a government application, however, the government may appeal to the FISA Court of Review, which is also fallible and therefore will sometimes erroneously overturn a FISA judge's (appropriate) denial of a surveillance order. In other words, the asymmetrical appeals system is more likely to produce false positives (granting surveillance orders that should not have been granted) than to suffer from false negatives (denying a surveillance order that should have been granted).

---

281. *See supra* text accompanying notes 186–87.

282. *See* Aziz Z. Huq, *Forum Choice for Terrorism Suspects*, 61 DUKE L.J. 1415, 1464–66 (2012) (explaining how systems of sequential decision making can lead to more false positives than false negatives).

Limiting appeals to the government might also have the effect of pushing the development of the law in the government's favor.[283] A FISA judge can avoid generating appeals and the concomitant possibility of reversal by granting the government's order. This means that even eliminating all other possible causes of progovernment bias, the judges have incentives to grant all plausible surveillance orders. Thus the applications that are denied and appealed will represent the most aggressive government surveillance efforts. Sometimes the appeals court will also deny that application. But sometimes it may grant it, thereby expanding the scope of permissible surveillance operations. As this process repeats itself over time, surveillance authorities will therefore slowly grow broader. Of course, so far as we know, the FISA Court of Review is rarely asked to review denied applications (probably because there are almost none), so the process in this context would be very slow indeed. It is, nevertheless, a likely result of limiting appeals to the government.

Again, the USA FREEDOM Act adopted a toothless solution to this problem. It provides that the FISA Court "shall certify for review to the [FISA Court of Review] any question of law . . . that the court determines warrants such review because of a need for uniformity or because . . . [it] would serve the interests of justice."[284] This provides a mechanism for judicial review of FISA judge rule-making decisions that the government does not control. The Act should, however, have granted the amicus the right to request reconsideration of FISA Court decisions as well, to appeal FISA Court or FISA Court of Review decisions, and to participate in those appeals.[285] An adversarial process with no power to appeal is not a true adversarial process. If the amicus's role is to represent the interests of the American people, we must establish a system that allows her to do so at her own discretion and at all states of litigation, rather than leaving it to the court.

3. Transparency

FISA Court critics proposed several ways to increase the transparency of the court's operations and opinions. Transparency of judicial decisions is critical for oversight of the government generally, including oversight of the courts. Had the court's opinions interpreting the meaning of "relevant" in the pen/trap statute and section 215 been public when they were initially issued, the USA FREEDOM Act itself might have passed years ago. Indeed, one only needs to look at the impetus for

---

283. This argument is derived from Professor Jonathan Masur's assessment of the patent application process. Jonathan Masur, *Patent Inflation*, 121 YALE L.J. 470 (2011); *see also* Huq, *supra* note 283, at 1467–68 (applying Masur's argument to the context of terrorism detention decisions).

284. USA FREEDOM Act of 2015, Pub. L. No. 114-23, sec. 401, § 103(j), 129 Stat. 268, 280–81 (to be codified at 50 U.S.C. § 1803).

285. Other proposals were more in line with the original version of the USA FREEDOM Act. *See* PCLOB SECTION 215 REPORT, *supra* note 34, at 187–88 (agreeing that more opportunity for appellate review is desirable and that the advocate should have a role in calling for review). At the opposite end of the spectrum, the Constitution Project, a nonpartisan think tank, argues that all FISA Court decisions should be automatically subject to appellate review. Constitution Project Letter, *supra* note 256.

the recent public and legislative debate over surveillance—massive leaks of secret information, including secret FISA Court orders and opinions—to recognize the way in which transparency promotes accountability and more thoroughly vetted policy. Making judicial decisions available to the public exposes flawed or unpersuasive rulings as well as potentially undesirable developments in the law. Some of the proposals for increased transparency were aimed at informing the public at large. Others were designed to ensure that Congress—or some portion of Congress, such as its intelligence committees—is sufficiently informed to facilitate its own oversight activities.

The USA FREEDOM Act attempted to address transparency in both the public and congressional contexts. Section 602 of the Act provides that the Director of National Intelligence and the Attorney General "shall conduct a declassification review of each decision, order, or opinion issued by the [FISA Court or the FISA Court of Review] that includes a significant construction or interpretation of any provision of law . . . [and] make publicly available to the greatest extent practicable each such decision, order, or opinion."[286] This provision will make more FISA Court opinions that engage in rule making available to the public. And while FISA already required that the Attorney General report all opinions that include significant construction or interpretation of FISA to the congressional intelligence oversight committees,[287] another section of the USA FREEDOM Act ensures that those opinions also promptly make their way to Congress.[288]

These provisions, while promising, suffer from flaws similar to the amicus and the appeals provisions. As with oversight of any classified or otherwise secret operations, there is a fundamental tension between transparency and intelligence collection.[289] Because they are responsible for maximizing intelligence collection effectiveness, members of the intelligence community itself cannot serve as independent arbiters of what should be made public. They will tend to value intelligence over transparency, and they will tend to have extremely low tolerance for any risk that transparency might pose. The USA FREEDOM Act, however, assigns to executive branch officials the decision whether an opinion qualifies for being made publicly available—that is, whether it is a "significant construction or interpretation of any provision of law."[290] Moreover, the Act requires that the Director of National Intelligence and the Attorney General make FISA Court

---

286. USA FREEDOM Act of 2015, Pub. L. No. 114-23, Sec. 402, § 602(a), 129 Stat. 268, 281 (to be codified at 50 U.S.C. § 1872).

287. 50 U.S.C. § 1871(a)(5) (2012); USA FREEDOM Act of 2015, Pub. L. No. 114-23, sec. 604, § 601(c)(1), 129 Stat. 268, 297 (to be codified at 50 U.S.C. § 1871). Some proposals went further, calling for public access to all FISA Court opinions—fully, in redacted form, or by summary—that interpret the scope, meaning, or constitutionality of FISA. *The Administration's Use of FISA Authorities: Hearing Before the H. Comm. on the Judiciary*, 113th Cong. 16 (2013) (written statement of Jameel Jaffer, ACLU Deputy Legal Director, and Laura W. Murphy, Director, ACLU Washington Legislative Office).

288. Sec. 604, § 601(c)(1), 129 Stat. 268, 297.

289. *Cf., e.g.*, Emily Berman, *Regulating Domestic Intelligence Collection*, 71 WASH. & LEE L. REV. 3 (2014).

290. Sec. 402(a)(2), § 602(b), 129 Stat. at 281 (to be codified at 50 U.S.C. § 1872).

opinions publicly available only "to the greatest extent practicable."[291] In addition, the Director of National Intelligence may waive the declassification requirement altogether if "necessary to protect the national security of the United States or properly classified intelligence sources or methods."[292] These exceptions are likely to swallow the rule.

Another flaw in the USA FREEDOM Act transparency provision is that it is limited to FISA Court decisions, orders, and opinions. There may be instances in which true transparency calls for additional documents to be released—submissions to the court, for example, or transcripts of proceedings.

4. Promoting the FISA Court's Use of Technical Expertise

Another meaningful step toward ensuring a more effective rule making performance by the FISA Court—and one that the USA FREEDOM Act partially embraced—is to ensure that FISA judges have access to increased technical expertise. The NSA's surveillance programs make use of the latest, cutting-edge technology. This technology is complex and constantly evolving. Indeed, some of the compliance issues that the NSA experienced have stemmed from the fact that "from a technical standpoint, there was no single person [at the NSA] who had a complete technical understanding of the . . . system architecture."[293] Moreover, compliance measures are more and more frequently built into the surveillance programs themselves as filters, or limits on searches, or firewalls on access to particular databases. Software fixes, for example, sought to prevent queries using non-RAS-approved identifiers after the NSA discovered that non-RAS-approved queries were accessing the metadata databases.[294] Judges need to be aware of the oversight opportunity that such software-based mechanisms present, as well as their limitations. Thus to fully understand both the programs it is overseeing and whether existing compliance or minimization procedures are going to be effective in carrying out the court's orders, the court must be able to understand and assess complex surveillance technology and software.[295]

The USA FREEDOM Act—consistent with recommendations from both the President's Review Group[296] and the PCLOB[297]—took one step to improve the

---

291. *Id*. sec. 402(a)(2), § 602(a), 129 Stat. at 281.

292. *Id*. sec. 402(a)(2), § 602(c), 129 Stat. at 281.

293. Declaration of Lieutenant General Keith B. Alexander at 18–19, *In re* Production of Tangible Things from [REDACTED], No. BR 08-13 (Feb. 13, 2009).

294. Supplemental Declaration of Lieutenant General Keith B. Alexander at 9–10, United States Army, Director of the National Security Agency, *In re* Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 25, 2009).

295. PRESIDENT'S REVIEW GRP. REPORT, *supra* note 43, at 205 (asserting that "the FISC should be able to call on independent technologists . . . who do not report to NSA or Department of Justice"); *see also* Laura K. Donohue, *FISA Reform*, 10 I/S: J.L. & POL'Y INFO. SOC'Y 599, at 626–27 (2014) (arguing that the FISA Court needs a science and technology expert "to help the court to understand new and emerging technologies").

296. PRESIDENT'S REVIEW GRP. REPORT, *supra* note 43, at 205 (recommending that the FISA Court be able to call upon independent technologists).

297. PCLOB SECTION 215 REPORT, *supra* note 34, at 184–89 (recommending that the FISA

court's available expertise. Section 402 of that Act facilitates increased access to technical expertise by providing that the court "may appoint an individual or organization to . . . provide technical expertise, in any instance as such court deems appropriate."[298] As with the amicus provision, however, this gives the Court no authority that it did not already have under its inherent powers. Perhaps Congress's suggestion to make use of this power will make FISA judges more likely to do so, but it is unclear that this provision will result in actual change.

I would suggest an additional measure toward promoting expertise: removing the term limit for FISA judges. To the extent there is a shortfall of technical knowledge on the court, it is compounded by the way the court operates. First, recall that each judge may serve only one seven-year term. So after accumulating seven years' worth of expertise on both the complicated legal regime governing FISA and the technology implementing that regime, one FISA judge is replaced by another who lacks this expertise. Similar concerns about personnel turnover sapping expertise prompted the abolition of term limits on the Senate Select Committee on Intelligence.[299] Just as members of Congress develop expertise in the issues over which the committees on which they sit exercise jurisdiction, FISA judges develop expertise in their time on the court. This expertise should be retained rather than dismissed.

A final thought on boosting the FISA Court's rule-making chops. It is not clear that encouraging the court to parse more carefully the government's bulk-collection arguments will result in a net increase in privacy protections. To be sure, it might result in a more narrowly conscribed interpretation of FISA, but that is not the same thing. When one route of intelligence collection is limited, the government has often implemented alternatives that might yield even larger losses in privacy. When the Bush Administration felt too constrained by FISA in the wake of 9/11, for example, it implemented the Terrorist Surveillance Program, a new, secret program with broader surveillance authority than even the most forgiving interpretation of FISA provided.[300] Similarly, on a more granular level, when the FBI has been refused individual section 215 orders, it has at times acquired the same information through the use of National Security Letters (a form of administrative subpoena), which do not have the benefit of any judicial oversight.[301] So we must acknowledge the possibility that denial of statutorily approved surveillance might result in a similar

---

Court both take advantage of its inherent power to appoint technical experts to assist it in reviewing voluminous or technical materials and amend its rules to allow that, when faced with difficult technological questions, FISA judges can "call upon outside lawyers . . . to offer analysis of legal or technical issues").

298. USA FREEDOM Act of 2015, Pub. L. No. 114-23, sec. 401, § 103(i)(2)(B), 129 Stat. 268, 279 (to be codified at 50 U.S.C. § 1803).

299. *See* S. RES 445, 108th Cong. (2004) (enacted); NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, 9/11 COMMISSION REPORT 421 (2004) ("Members should serve indefinitely on the intelligence committees, without set terms, thereby letting them accumulate expertise.").

300. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html [https://perma.cc/5BCT-NQSS].

301. *See supra* note 93 and accompanying text.

form of surveillance, though less transparent and less-fully supervised, under executive authority.

CONCLUSION

As the FISA Court approaches its fourth decade, it is being asked to do more than ever before, and certainly more than Congress envisioned for it in 1978. Looking at the different roles the court now plays makes plain that the magnitude of the post 9/11 changes assigning to the court rule-making responsibilities has been underappreciated. The USA FREEDOM Act sought to address some of the court's rule-making deficiencies. Its minor modifications to the court's proceedings, however, fail to account for the unique challenges of rule-making and are therefore doomed to fail. Moreover, Congress passed up a prime opportunity to render even more effective the court's already laudable gatekeeping activities by focusing on the flow of information from the executive to the FISA Court.