REFORMING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT'S INTERPRETIVE SECRECY PROBLEM

GREGORY S. MCNEAL*

On June 5, 2013, *The Guardian* published excerpts from classified documents that were stolen from the National Security Agency (NSA) by former contractor Edward Snowden.[1] The disclosures set off the publication of a series of articles revealing various classified programs at the NSA. Of particular interest to commentators were the section 215 metadata collection program, which allowed the FBI and NSA to gather the telephone records of nearly all Americans, and the section 702 surveillance program, which allowed for the collection of the contents of certain foreign-located non-U.S. persons' electronic communications.[2]

While the technical details of each of the programs differ, perhaps the most substantial difference between the two programs is that the legal authority upon which the section 702 surveillance program rests left observers with little doubt as to the scope of the program—in fact, Congress had publicly debated the scope of that program.[3] The section 215 metadata collection program, on the other hand, relied upon a secret legal interpretation that was far more expansive than the statutory text upon

---

* Gregory S. McNeal, J.D., Ph.D., Associate Professor of Law, Pepperdine University School of Law. This essay was adapted from remarks given at the 2014 Federalist Society Annual Student Symposium at the University of Florida in Gainesville, Florida.

1. Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [http://perma.cc/8NMB-CSKX].

2. *See, e.g.*, Stephen I. Vladeck, *Big Data Before And After Snowden*, 7 J. NAT'L SECURITY L. & POL'Y 333, 334–35 (2014); Amy Davidson, *The N.S.A.-Verizon Scandal*, THE NEW YORKER, June 6, 2013, http://www.newyorker.com/news/amy-davidson/the-n-s-a-verizon-scandal [http://perma.cc/3MUW-PPXL].

3. 158 CONG. REC. 122,5890–5900 (2012); 154 CONG. REC. 11,227–71 (2007).

which the program relied.[4] This essay argues that such interpretive secrecy should be reformed. Specifically, this essay argues that all opinions of the Foreign Intelligence Surveillance Court (FISC) that engage in substantial legal interpretations or constructions should be subject to automatic review by the Foreign Intelligence Surveillance Court of Review (FISCR). Further, this essay argues that all opinions of the FISC which engage in substantial legal interpretations or constructions should be presumptively public, with appropriate redactions subject to automatic review by the FISCR.

While both the section 702 surveillance program and the section 215 metadata collection program were of popular interest, perhaps the more controversial of the two programs was the section 215 metadata collection program. Why? There are a few explanations. First, the section 702 program focused exclusively on non-U.S. persons, while the section 215 program focused almost exclusively on U.S. persons. That fact may have heightened civil liberties concerns associated with the program—especially among Americans who may be okay with spying on foreigners, but not with spying directed at themselves. Second, the technical complexity associated with the section 702 program, which involved the foreign collection of electronic communications made by non-U.S. citizens overseas, stands in stark contrast to the section 215 program which could easily (albeit somewhat inaccurately) be described within the amount of text allowed for a tweet: "The NSA is collecting records of all phone calls made in the United States and is doing so without a warrant." Third, the section 702 program was deemed an essential counterterrorism tool that resulted in actual thwarted plots and other successful counterterrorism operations, whereas the section 215 program did not have any success stories (measured by thwarted plots) that its advocates could point to as a justification for collecting records on all Americans.[5]

---

4. Charlie Savage, *Public Said to Be Misled on Use of the Patriot Act*, N.Y. TIMES, Sept. 21, 2011, http://www.nytimes.com/2011/09/22/us/politics/justice-dept-is-accused-of-misleading-public-on-patriot-act.html [http://perma.cc/XB2Q-JHEV].

5. Courtney Kube, *NSA chief says surveillance helped foil 54 plots*, NBC NEWS (Jun. 27, 2013, 6:04 PM), http://usnews.nbcnews.com/_news/2013/06/27/19175466-nsa-chief-says-surveillance-programs-helped-foil-54-plots# [http://perma.cc/47E4-AVYY] (noting that the government claimed success based on both programs, but only listing specific examples from the 702 program).

This essay will focus mostly on a fourth explanation for the wide opposition to the section 215 program: democratic legitimacy. The legal foundation for the section 702 program was widely debated in Congress. Members of Congress, advocacy groups, and the public were aware (or at least had the opportunity to make themselves aware) of the scope of the program, which was based in large part on the Terrorist Surveillance Program. Contrast that record of public debate with the section 215 program, which relied upon a broad interpretation of a statute. That interpretation was argued in secret, issued in secret, not subject to appellate review, and not disclosed to members of Congress while they were debating whether the statute enabling the section 215 program should be renewed. This lack of democratic transparency is a significant failure of the FISA Court system, which should be remedied.

This essay proceeds as follows: First, I will provide an overview and history of the section 215 program and the section 702 program. Next, I will suggest that interpretive secrecy can be remedied by mandating appellate review of FISC opinions and orders and by imposing a requirement that all FISC opinions and orders are presumptively published, subject to appropriate redactions.

I. HISTORY OF AND PUBLIC DEBATE ABOUT SECTION 702 OF FISA

Following the September 11th attacks, President George W. Bush issued an order authorizing the NSA to collect the contents of certain international electronic communications.[6] The program allowed warrantless electronic surveillance within the U.S. The ostensible goal of the program was to prevent acts of terrorism. Under President Bush's order, the NSA was permitted to "collect: (1) the contents of certain international communications, a program that was later referred to as the Terrorist Surveillance Program ('TSP')" and (2) collect in bulk non-

6. Press Release, Office of the Dir. of Nat'l Intelligence, DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001 (Dec. 21, 2013), http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/991-dni-announces-the-declassification-of-the-exisitence-of-collection-activities-authorized-by-president-george-w-bush-shortly-after-the-attacks-of-september-11,-2001 [http://perma.cc/TKH8-5EWN] [hereinafter DNI Press Release].

content information, or "metadata," about telephone and Internet communications—a program that later evolved into the section 215 program discussed in the next section.[7] The two programs combined, and "[t]he collection of communications content and bulk metadata under these presidential authorizations became known as the President's Surveillance Program."[8] According to a 2009 report by the inspectors general of several defense and intelligence agencies, over time, "the program became less a temporary response to the September 11 terrorist attacks and more a permanent surveillance tool."[9]

The TSP became a national news story when, in December 2005, the *New York Times* published articles revealin that the NSA was intercepting the contents of international communications.[10] President Bush confirmed the existence of the programs and defended them in a White House speech in which he pledged to continue the surveillance, arguing the program was essential to national security.[11] The Assistant Attorney General also wrote a letter to the Senate Select Committee on Intelligence, defending the program:

> As described by the President, the NSA intercepts certain international communications into and out of the United States of people linked to al Qaeda or an affiliated terrorist organization. The purpose of these intercepts is to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States. The President

---

7. *Id.*

8. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 16 (2014), *available at* http://www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report-PRE-RELEASE.pdf [http://perma.cc/N42L-H4HM] [hereinafter PCLOB 702].

9. *Id*. at 16–17 (quoting OFFICES OF THE INSPECTORS GEN. OF THE DEP'T OF DEF. ET AL., UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 31 (2009)).

10. 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/16program.html?pagewanted=all [http://perma.cc/5LHR-FCSW]; Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES, Dec. 24, 2005, http://www.nytimes.com/2005/12/24/politics/24spy.html?emc=eta1&_r=0 [http://perma.cc/6WX7-N45L].

11. David E. Sanger, *Bush Says He Ordered Domestic Spying*, N.Y. TIMES, Dec. 18, 2005, http://www.nytimes.com/2005/12/18/politics/18bush.html?pagewanted=all [http://perma.cc/BN83-B75Q].

> has made clear that he will use his constitutional and statutory authorities to protect the American people from further terrorist attacks, and the NSA activities the President described are part of that effort. Leaders of the Congress were briefed on these activities more than a dozen times.
>
> The purpose of this letter is to provide an additional brief summary of the legal authority supporting the NSA activities described by the President.
>
> As an initial matter, I emphasize a few points. The President stated that these activities are "crucial to our national security." The President further explained that "the unauthorized disclosure of this effort damages our national security and puts our citizens at risk. Revealing classified information is illegal, alerts our enemies, and endangers our country." These critical national security activities remain classified. All United States laws and policies governing the protection and nondisclosure of national security information, including the information relating to the activities described by the President, remain in full force and effect. The unauthorized disclosure of classified information violates federal criminal law. The Government may provide further classified briefings to the Congress on these activities in an appropriate manner. Any such briefings will be conducted in a manner that will not endanger national security.[12]

To defend the legality of the program, the Department of Justice also issued a white paper explaining the legal justifications supporting surveillance.[13]

> The NSA activities are consistent with the preexisting statutory framework generally applicable to the interception of communications in the United States—the Foreign Intelligence Surveillance Act ("FISA"), as amended, 50 U.S.C. §§ 1801-1862 (2000 & Supp. II 2002), and relevant related provisions in chapter 119 of title 18. Although FISA generally requires judicial approval of electronic surveillance, FISA also contemplates that Congress may authorize such surveillance

---

12. Letter from William E. Moschella, Assistant Att'y Gen., to The Honorable Pat Roberts, Chairman, Senate Select Committee on Intelligence, et al. (Dec. 22, 2005), *available at* http://www.fas.org/irp/agency/doj/fisa/doj122205.pdf [http://perma.cc/PQ7A-SJS4].

13. U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (2006), *available at* http://epic.org/privacy/terrorism/fisa/doj11906wp.pdf [http://perma.cc/A5QT-2WQJ].

> by a statute other than FISA. See 50 U.S.C. § 1809(a) (prohibiting any person from intentionally "engag[ing] . . . in electronic surveillance under color of law except as authorized by statute"). The AUMF, as construed by the Supreme Court in *Hamdi* and as confirmed by the history and tradition of armed conflict, is just such a statute. Accordingly, electronic surveillance conducted by the President pursuant to the AUMF, including the NSA activities, is fully consistent with FISA and falls within category I of Justice Jackson's framework.
>
> Even if there were ambiguity about whether FISA, read together with the AUMF, permits the President to authorize the NSA activities, the canon of constitutional avoidance requires reading these statutes in harmony to overcome any restrictions in FISA and Title III, at least as they might otherwise apply to the congressionally authorized armed conflict with al Qaeda. Indeed, were FISA and Title III interpreted to impede the President's ability to use the traditional tool of electronic surveillance to detect and prevent future attacks by a declared enemy that has already struck at the homeland and is engaged in ongoing operations against the United States, the constitutionality of FISA, as applied to that situation, would be called into very serious doubt. In fact, if this difficult constitutional question had to be addressed, FISA would be unconstitutional as applied to this narrow context. Importantly, the FISA Court of Review itself recognized just three years ago that the President retains constitutional authority to conduct foreign surveillance apart from the FISA framework, and the President is certainly entitled, at a minimum, to rely on that judicial interpretation of the Constitution and FISA.
>
> Finally, the NSA activities fully comply with the requirements of the Fourth Amendment. The interception of communications described by the President falls within a well-established exception to the warrant requirement and satisfies the Fourth Amendment's fundamental requirement of reasonableness. The NSA activities are thus constitutionally permissible and fully protective of civil liberties.[14]

While the White House and Department of Justice publicly proclaimed that the TSP was essential for national security and stood on strong legal footing, the government nevertheless sought authorization under FISA to conduct the content collec-

---

14. *Id.*at 2–3.

tion that had been occurring under the executive orders that constituted the TSP.[15]

A declassified certification before the FISC reveals what the government was authorized to collect as of January 2007. In that Attorney General's certification, which the FISC authorized, the government was permitted to conduct electronic surveillance of telephone and internet communications at specific communication facilities, only after the government made a probable cause determination regarding one of the communicants, and if the email addresses and telephone numbers to be monitored were reasonably believed to be used by persons located outside the United States.[16] This order later became known as the "Foreign Telephone and Email Order" and was modified in May 2007, shifting responsibility for the probable cause determination from the government to the FISC.[17] The government believed that the modified order created an "intelligence gap" and "degraded [intelligence] capabilities."[18] To close the gap, the government began using the authorities then in place under the FISA statute to "obtain individual court orders to compel private companies to assist the government in acquiring the communications of individuals located overseas who were suspected of engaging in terrorism and who used United States–based communication service providers."[19] Such individual applications were onerous and, in the words of Assistant Attorney General for National Security, Kenneth Wainstein, resulted in the use of "considerable resources" on the part of the FISC and the government.[20] "Drafting applications

---

15. DNI Press Release, *supra* note 6.

16. Declassified Certification of Attorney General Michael B. Mukasey at ¶ 37, *In re* Nat'l Sec. Agency Telecomms. Records Litig., 564 F. Supp. 2d 1109 (N.D. Cal. 2008) (No. 06-1791-VRW), *available at* http://www.dni.gov/files/documents/0505/AG Mukasey 2008 Declassified Declaration.pdf [http://perma.cc/PAC8-GRJ8].

17. PCLOB 702, *supra* note 8, at 17.

18. *See* S. REP. NO. 110–209, at 5, 31 (2007), *available at* http://www.gpo.gov/fdsys/pkg/CRPT-110srpt209/pdf/CRPT-110srpt209.pdf [http://perma.cc/VZ75-Q57R]; Eric Lichbtlau, James Risen & Mark Mazzetti, *Reported Drop in Surveillance Spurred a Law*, N.Y. TIMES, Aug. 11, 2007, http://www.nytimes.com/2007/08/11/washington/11nsa.html?pagewanted=all [http://perma.cc/FMD8-VVYX].

19. PCLOB 702, *supra* note 8, at 18.

20. *The Need to Bring the Foreign Intelligence Surveillance Act Into the Modern Era: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 6 (2007) (statement of Kenneth L. Wainstein, Assistant Att'y Gen. of the United States), available at

that demonstrated satisfaction of this probable cause standard, the government has asserted, slowed and in some cases prevented the acquisition of foreign intelligence information."[21]

"The collection of communications content pursuant to presidential authorization ended in January 2007 when the U.S. Government transitioned the TSP to the authority of the FISA" and judicial supervision by court orders under the FISC.[22] Because of the inefficiencies in obtaining FISC approval for surveillance, the Bush Administration proposed modifications to FISA:

> Reports by the Director of National Intelligence to Congress that implementation of the FISC's May 2007 modifications to the Foreign Telephone and Email Order had resulted in 'degraded' acquisition of communications, combined with reports of a 'heightened terrorist threat environment,' accelerated Congress' consideration of these proposals.[23]

The surveillance programs first conducted pursuant to executive orders, then under judicial supervision by the FISC, were largely endorsed by Congress in August 2007 in a temporary measure known as the Protect America Act (PAA), which was permanently replaced by the FISA Amendments Act of 2008.[24]

The FISA Amendments Act of 2008 was substantially debated, and ultimately replaced the expired provisions with the new section 702 of FISA. "In addition to Section 702, the FISA Amendments Act of 2008 also enacted Sections 703 and 704 of FISA, which required judicial approval for targeting U.S. persons located abroad in order to acquire foreign intelligence information."[25]

II. WHAT IS SECTION 702 SURVEILLANCE?

As mentioned earlier, section 702 surveillance is inherently complex, made even more complex by the fact that it is part of a broader body of law, the Foreign Intelligence Surveillance Act, which is itself complex. The Privacy and Civil Liberties

---

http://www.intelligence.senate.gov/070501/wainstein.pdf [http://perma.cc/8BQW-K8SK].

21. PCLOB 702, *supra* note 8, at 18.

22. DNI Press Release, *supra* note 6.

23. PCLOB 702, *supra* note 8, at 19.

24. *Id.* at 17–20.

25. PCLOB 702, *supra* note 8, at 20.

Oversight Board (PCLOB) attempted to summarize the statutory scope of section 702 as follows:

> Section 702 of FISA permits the Attorney General and the Director of National Intelligence to jointly authorize the (1) targeting of persons who are not United States persons, (2) who are reasonably believed to be located outside the United States, (3) with the compelled assistance of an electronic communication service provider, (4) in order to acquire foreign intelligence information. Each of these terms is, to various degrees, further defined and limited by other aspects of FISA. Congress also imposed a series of limitations on any surveillance conducted under Section 702. The statute further specifies how the Attorney General and Director of National Intelligence may authorize such surveillance, as well as the role of the FISC in reviewing these authorizations.[26]

The PCLOB's short summary and analysis is based on the statutory language, which while complex is known to congressional drafters and is readily discernible by anyone seeking to understand section 702 authorities.

Section 702 authorizes the targeting of persons, and persons are defined in FISA. Persons are not only individuals, but also groups, entities, associations, corporations, or foreign powers.[27] As the PCLOB noted, the "definition of 'person' is therefore broad, but not limitless: a foreign government or international terrorist group could qualify as a 'person', but an entire foreign country cannot be a 'person' targeted under Section 702."[28] Surveillance under section 702 may not intentionally target U.S. persons.[29] To ensure that only the appropriate people are being targeted by the NSA, the agency uses selectors "such as email addresses and telephone numbers. The NSA must make determinations (regarding location, U.S. person status, and foreign intelligence value) about the users of each selector on an individualized basis. It cannot simply assert that it is targeting a particular terrorist group."[30] Pursuant to the terms of the statute, the non-U.S. persons targeted by the NSA must be "reasonably be-

---

26. *Id.*
27. 50 U.S.C. § 1801(m) (2012).
28. PCLOB 702, *supra* note 8, at 21.
29. *Id.*
30. *Id.*

lieved to be located outside the United States."[31] The statute authorizes the government to compel "electronic communication service provider[s]" to assist the government in targeting non-U.S. persons reasonably believed to be located outside the United States.[32] Finally, the statute makes clear that the purpose for which non-U.S. persons are to be targeted is "to acquire foreign intelligence information."[33] Further, the government cannot use "what is generally referred to as 'reverse targeting,' which would occur if the government were to intentionally target persons reasonably believed to be located outside the United States 'if the purpose of the acquisition is to target a particular, known person reasonably believed to be in the United States.'"[34]

Thus, while the statutory language is dense, one could know upon examining section 702 (and the rest of FISA) who the government was authorized to surveil, what the government was authorized to collect, where the collection was to take place, and for what purpose. The scope of communications swept up under section 702 authorities is no doubt extensive, but the authority to engage in such surveillance was known to Congress at the time it enacted the provisions of section 702. This legal history stands in contrast to the bulk metadata collection conducted pursuant to section 215, the subject of the next section.

III. SECTION 215 INTERPRETIVE OPACITY MAKES FOR A MORE CONTROVERSIAL PROGRAM

As mentioned in the previous section, shortly after the September 11 attacks, President Bush issued executive orders authorizing certain intelligence collection activities. One component of those executive orders was the bulk collection of non-content information about telephone communications. As was discussed in the previous section, *The New York Times*'s revelations about parts of the President's Surveillance Program compelled the government to seek approval from the FISC for portions of that program. Similarly, the government "moved to transition the telephone records program from the President's

31. 50 U.S.C. § 1881b(b)(1) (2012).
32. *Id.* § 1881a(g)(2)(A)(vi).
33. *Id.* § 1881a(g)(2)(A)(v).
34. PCLOB 702, *supra* note 8, at 23 (citing 50 U.S.C. § 1881a(b)(2)).

Surveillance Program to a section of FISA known as the 'business records' provision."[35] The business records provision of FISA, formally titled "Access to certain business records for foreign intelligence and international terrorism investigations," originally permitted the FBI to apply to the FISA court for an order requiring a business "to release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism." Any application for such an order was required to attest "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."[36]

Section 215 of the PATRIOT Act "significantly extended the reach of FISA's business records provision" by expanding the FBI's authority to seek records to "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism."[37] The PATRIOT Act also enabled the FBI to acquire such records merely by specifying that such records were "'for an authorized investigation' conducted under guidelines approved by the Attorney General," thus abandoning the statutory requirement for the FBI to demonstrate "specific and articulable facts" to show "that a person to whom the records pertained was a foreign power or an agent of a foreign power."[38] Notably, the Attorney General's guidelines for investigations are an internal document, portions of which have been made public in declassified form, however the guidelines are subject to change at the discretion of the Attorney General and need not be made public. Thus, this change not only modified the substance of the government's information gathering authority, but also the transparency of the authority.

---

35. PRIVACY AND 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 40 (2014), *available at* http://www.pclob.gov/All Documents/Report on the Telephone Records Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf [http://perma.cc/3W8H-FDCG?type=pdf] [hereinafter PCLOB 215].

36. *Id.* at 40–41.

37. *Id.* at 41 (citing § 1861(a)(1)).

38. *Id.* (citing § 1861(b)(2)).

Section 215, along with other provisions of the PATRIOT Act, were set to expire unless reauthorized by Congress. Accordingly debates in Congress took place beginning in 2005 and extending into the spring of 2006.[39] These debates over the "reauthorization of Section 215, including proposals to limit its scope and impose additional safeguards" were "occurring at the same time that executive branch lawyers were formulating a strategy to use that statute as the legal basis for the NSA's bulk telephone records collection."[40]

Importantly, the collection of telephone records under the President's Surveillance Program was a classified program that was not revealed by the 2005 story in *The New York Times* or in the President's speeches defending the TSP, or in the white paper defending the administration's surveillance programs. Thus, while section 215 of the PATRIOT Act was being debated, the government's plans to seek new legal authority for that collection were not made public. Thus, congressional debates about the terms on which section 215 should be renewed included no public discussion of the fact that the executive branch was planning to place the NSA's bulk calling records program under the auspices of the reauthorized statute.[41]

The USA PATRIOT Improvement and Reauthorization Act of 2005 was signed into law in March 2006.[42] The law changed section 215, which includes the business records provision of FISA. A new provision was added that required the FISC to determine that when the government sought records, those records were likely "relevant" to an FBI investigation. Such a showing would be made through an application that contained "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment)."[43]

The law further limited what could be obtained under an order to produce a "tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United

---

39. PCLOB 215, *supra* note 35, at 41.

40. *Id.*

41. *Id.* at 41.

42. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006).

43. 50 U.S.C. § 1861(b)(2)(A) (2012).

States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things."[44]

Thus while Congress had publicly debated section 215, seemingly believing that the authority under the so-called "business records" or "library records" provision had been narrowed, the legislature was unaware of the government's efforts to substantially expand collection of records under section 215. In a legal memo submitted before the FISC on May 23, 2006, government lawyers requested that the FISC direct certain U.S. telephone companies to provide the NSA with telephone call records in the possession of specific telephone companies.[45] Moreover, the government's request asked the court to compel the companies to produce the records on an ongoing daily basis for a period of ninety days.[46]

Thus, despite statutory language that seemed to limit the use of section 215 to specific items, relevant to an FBI investigation, that could only be obtained with a subpoena or a court order, the government instead was requesting the court order telephone companies to hand over all of their call records for a ninety day period. As the discussion above made clear, section 215 required "a statement of facts showing that there are reasonable grounds to believe" that the records sought "are relevant to an authorized investigation."[47] The government admitted that it would be collecting records in bulk, stating:

> The collection sought here will make possible a potentially powerful tool that the Government has to discover enemy communications: metadata analysis. For telephone calls, metadata essentially consists of routing information that includes the telephone number of the calling party, the tele-

---

44. *Id*. § 1861(c)(2)(D).

45. Memorandum of Law in Support of Application for Certain Tangible Things for Investigations to Protect Against International Terrorism, *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 23, 2006), *available at* http://www.clearinghouse.net/chDocs/public/NS-DC-0009-0004.pdf [http://perma.cc/GFS4-QHSZ] [hereinafter Memo in Support].

46. *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. 2013).

47. 50 U.S.C. § 1861(b)(2)(A).

> phone number of the called party, and the date, time and duration of the call. It does not include the substantive content of the communication or the name, address, or financial information of a subscriber or customer. Relying solely on such metadata, the Government can analyze the contacts made by a telephone number reasonably suspected to be associated with a terrorist, and thereby possibly identify other, previously unknown, terrorists. The primary advantage of metadata analysis as applied to telephony metadata is that it enables the Government to analyze past connections and patterns of communication. That analysis is possible, however, only if the Government has collected and archived a broad set of metadata that contains within it the subset of communications that can later be identified as terrorist-related.[48]

Moreover, the government recognized that not all records would be relevant to an investigation, but justified relevance on what could best be described as usefulness or necessity to enable the government's metadata analysis, stating:

> The Application fully satisfies all requirements of title V of FISA. In particular, the Application seeks the production of tangible things "for" an international terrorism investigation. 50 U.S.C. § 1861(a)(1). In addition, the Application includes a statement of facts demonstrating that there are reasonable grounds to believe that the business records sought are "relevant" to an authorized investigation. *Id.* § 1861(b)(2). Although the call detail records of the [redacted] contain large volumes of metadata, the vast majority of which will not be terrorist-related, the scope of the business records request presents no infirmity under title V. All of the business records to be collected here are relevant to FBI investigations into [redacted] because the NSA can effectively conduct metadata analysis only if it has the data in bulk.[49]

The government went even further, arguing that if the FISC found that the records were not relevant, that the FISC should read relevance out of the statute by tailoring its analysis in a way that would balance the government's request to collect metadata in bulk against the degree of intrusion into privacy interests. Disregarding the fact that the balancing of these in-

48. Memo in Support, *supra* note 45, at 1–2.
49. *Id.* at 2–3.

terests was likely already engaged in by Congress when writing section 215, the government wrote:

> In addition, even if the metadata from non-terrorist communications were deemed not relevant, nothing in title V of FISA demands that a request for the production of "any tangible things" under that provision collect *only* information that is strictly relevant to the international terrorism investigation at hand. Were the Court to require some tailoring to fit the information that will actually be terrorist-related, the business records request detailed in the Application would meet any proper test for reasonable tailoring. Any tailoring standard must be informed by a balancing of the government interest at stake against the degree of intrusion into any protected privacy interests. Here, the Government's interest is the most compelling imaginable: the defense of the Nation in wartime from attacks that may take thousands of lives. On the other side of the balance, the intrusion is minimal. As the Supreme Court has held, there is no constitutionally protected interest in metadata, such as numbers dialed on a telephone.[50]

Thus, what the government asked the court to disregard the judgment of the Congress as to the limitations and privacy interests at stake in the collection of business records. Specifically, the government asked the FISC to disregard Congress's imposition of a statutory requirement that business records be relevant, and in disregarding that statutory requirement rely on the fact that there was no constitutionally protected privacy interest in business records. The government's argument flipped the statute on its head, as the purpose of enhancing protections under section 215 was to supplement the constitutional baseline protections for privacy that were deemed inadequate by Congress.

Despite the problems associated with the government's request and legal analysis, FISC Judge Malcolm J. Howard signed an order approving the government's application.[51] The order did not provide an opinion explaining the legal analysis that supported the decision, rather the order merely recited the spe-

---

50. *Id.* at 3.

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

cific findings called for by section 215 and stated that the government's application satisfied those statutory requirements.[52] Because matters before the FISC are ex parte, the judge's order was not reviewed by the FISCR, and the order was kept secret from most members of Congress. Thus, a widely debated provision of the PATRIOT Act was used in a way never contemplated by members of Congress, and those members were left largely in the dark as to the new interpretation of the law.

IV. PROBLEMS WITH THE FISC'S STATUTORY ANALYSIS

The government cannot be faulted for following the system that was put into place by Congress, but the system is nevertheless faulty. Congress created a structure whereby the government can argue in an ex parte proceeding for an expansive interpretation of a statute, the initial application will only be reviewed by one judge, and that judge can issue an order in secret, without fearing appellate review or public rebuke. That system is destined to fail because it lacks democratic accountability. It is also suboptimal as it is bound to create poorly reasoned judgments and opinions.

The PCLOB's analysis and critique of the government's relevance arguments demonstrates how independent review of substantive decisions can yield more careful opinions. The PCLOB looked at the government's interpretation of relevance and wrote, "no case that we have found supports the interpretation of relevance embodied in the NSA's program."[53] Moreover, the PCLOB stated, "none of the government's arguments, in our view, supports a definition of 'relevant' as broad as the one the government proffers."[54] Examining the statutory requirement for relevance, the PCLOB wrote:

> First, had Congress wished to inscribe a standard of relevance in Section 215 even less exacting than those developed in analogous legal contexts, it could have done so. But contemporary statements from legislators, highlighted by the government itself, evince an intent to match Section 215 to

52. *Id*. at 3.
53. PCLOB 215, *supra* note 35, at 79.
54. *Id.*

> the standards used in those contexts. The reference to grand jury subpoenas added to the statute in 2006 was meant to reassure those with concerns about the scope of Section 215 that the statute was consistent with practice in other fields.[55]

This statement by the PCLOB is not remarkable on its face. In fact it is the type of analysis one would expect an opposing party to raise in court, or a judge to raise on appellate review. Thus it is remarkable that this argument did not occur to the FISC. But, when presented with only one side of an argument, and not fearing appellate review, one can understand how the FISC got their analysis wrong.

Furthermore, the PCLOB looked at the statutory "reasonable grounds to believe" standard, again engaging in basic statutory analysis of the type that an opposing party or appellate court would engage in. The PCLOB stated:

> By demanding only "reasonable grounds to believe," rather than certainty, that items sought are relevant to an investigation, the statute ensures that Section 215 is consistent with the analogous civil and criminal contexts—where the requester need not show that every item sought *actually* is relevant in an evidentiary sense, but merely that the items reasonably may be. The statute's reference to a reasonable *belief* about the items requested shows that it contemplates the same scenario faced in the subpoena and discovery arenas: the government seeks a category of items that it reasonably suspects, but cannot be sure, includes material pertinent to its investigation. That scenario, and the legal standards that govern it, still require some factual correlation between the category of documents defined by the government and the circumstances of the investigation for which they are sought.[56]

Again, the PCLOB engaged in statutory analysis, not complex legal reasoning. In so doing, it found that not only was the government's definition of relevance too expansive, but it also found that compelling providers to continuously hand over records to the government was also incompatible with the statutory text. While the PCLOB recognized the compelling nature of national security threats, such considerations in the view of the PCLOB did "not call for the wholesale elimination of rele-

---

55. *Id.* (footnotes omitted).
56. *Id.* at 79–80 (emphasis in original).

vance as a meaningful check on the government's acquisition of items."[57] In other words, the statutory protections Congress created (specifically relevance) were important to the statutory scheme Congress contemplated and that the public expects.

The PCLOB made reference to the statutory text and the changes Congress made to that text, noting in a footnote that:

> Congress amended Section 215 to clarify that there must be reasonable grounds to believe that records obtained under the statute are "relevant to" an investigation, not merely sought "for" an investigation; it further required "a statement of facts" supporting that belief . . . . It inserted the concept of "relevance" into the statute not to broaden it, but to reassure those with concerns that the statute was tethered to concepts well known in other areas.[58]

The PCLOB continued:

> No matter how critical national security investigations are, therefore, *some* articulable principle must connect the items sought to those investigations, or else the word "relevant" is robbed of meaning. Congress added a relevance requirement to Section 215 in 2006 knowing full well that the statute governs national security investigations. It cannot, therefore, have meant for the importance of such investigations to efface that requirement entirely.[59]

In light of this reasoning, how could the FISC have missed the ball on the statutory analysis of section 215? The problem is structural. When a court is presented with only one side of an argument, it is solely on that judge to get the argument right. One potential solution would be to have an independent advocate appear before the court. Another solution that can serve a similar function would be to require appellate review and presumptive transparency on all significant FISC opinions; presumptive appellate review is the subject of the next section.

---

57. *Id.* at 80–81.

58. *Id.* at 81 n.298 (internal citations omitted).

59. PCLOB 215, *supra* note 35, at 80–81 (emphasis in original).

V. INTERPRETIVE SECRECY AND THE NEED FOR TRANSPARENCY AND REVIEWABILITY

Interpretive secrecy is a significant problem in terms of democratic accountability. As Senator Ron Wyden once said, "secret operations and secret law are very different things . . . . Secret law is wrong. Our laws are supposed to be public."[60] That quote draws into focus the dividing line for determining the appropriateness of secrecy on the FISC. While there are good arguments for keeping matters before the FISC secret, secrecy must give way when a circumstance like that witnessed in the section 215 program results in unelected judges with life tenure interpreting laws in such a way that they go against the text of the law as written. Laws simply should not be interpreted in secret, without an opportunity for the public to know that the law that is on the books differs substantially from the law that is actually being used to justify a surveillance program. If the nation is to have democratic accountability, it requires appellate review of judgments and orders that do not comport with the law as it is written, and transparency regarding those judgments or orders. As the PCLOB stated in their review of the section 215 program:

> When a secret court accepts a counterintuitive reading of a law — one that could not possibly be guessed by reading the statutory language alone, and which invests the government with significant new powers — permitting congressional reenactment to enshrine that novel interpretation deprives the public of any ability to know that the law is, much less have any voice in changing it.[61]

In light of the problems outlined above, this essay makes two arguments. First, all FISC orders and opinions which rely upon or create a significant legal construction or interpretation should be subject to automatic de novo review by the FISCR. Second, all FISC orders and opinions should be presumptively public, subject to appropriate redactions, with such redactions

---

60. Joe Conason, *Senator Ron Wyden: How We Forced the NSA to Curtail Email Spying*, HUFFINGTON POST (July 31, 2013, 5:18 PM), http://www.huffingtonpost.com/joe-conason/ron-wyden-nsa-surveillance_b_3684480.html [http://perma.cc/J7ZT-HFXK] (quoting Senator Ron Wyden).

61. PCLOB 215, *supra* note 35, at 101–02.

automatically subject to de novo review by the FISCR. These two proposals will not solve all of the problems associated with the FISC, however they will serve to enhance the accountability of the FISC, will promote transparency, and will ensure better outcomes. It is axiomatic to suggest that when a judge knows that his or her opinion is subject to review and disclosure, he or she will write in a way to address all sides of an argument.

VI. A PROPOSED TRIGGER FOR PRESUMPTIVE REVIEW

FISA already includes a standard for "significant legal interpretations" albeit one for disclosure of matters before the FISC and FISCR to Congress, not one for presumptive appellate review; however that standard could be adopted to create a trigger for presumptive review of FISC opinions. The "significant legal interpretations" standard was written into law in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[62] That law required the Attorney General to provide a "summary of significant legal interpretations" of FISA "involving matters before" the FISC or the Court of Review.[63] The summary must include "interpretations presented in applications or pleadings filed with the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review by the Department of Justice."[64] The law requires disclosure of opinions or orders if they "include significant construction or interpretation" of FISA.[65]

This standard of "significant construction or interpretation" of FISA could be modified to become a trigger for appellate review by requiring that all opinions of the Foreign Intelligence Surveillance Court that involve significant construction or interpretation of *any statute or judicial precedent* are subject to de novo review by the Foreign Intelligence Surveillance Court of Review. Automatic review of lower court opinions is not unheard of in the national security cases. For example, in courts martial proceedings, trials that result in a conviction are auto-

62. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 601, 118 Stat. 3638 (2004).

63. 50 U.S.C. § 1871(a)(4) (2012).

64. *Id.*

65. *Id.* § 1871(a)(5).

matically reviewed by the convening authority, and the convening authority has discretion to mitigate the findings and sentence.[66] Furthermore, if the sentence imposed by the convening authority includes "death, dishonorable or bad—conduct discharge, or confinement for one year or more," the case is automatically reviewed by an intermediate court.[67] Those courts review cases for legal error, factual sufficiency and sentence appropriateness.

A de novo standard of review is appropriate for surveillance activities as it allows "multijudge panels that permit reflective dialogue and collective judgment" with regard to legal issues.[68] As the Supreme Court has explained, "[i]ndependent appellate review of legal issues best serves the dual goals of doctrinal coherence and economy of judicial administration," and while the Supreme Court was not speaking of surveillance, its admonitions regarding appellate review are perhaps stronger in the context of national security.[69]

However, national security surveillance oftentimes requires rapid action on the part of the courts; thus while this essay argues that FISC opinions should be presumptively reviewed, the order or opinion issued by the FISC should be immediately effective, and finalized pending review by the FISCR. A FISC judge should have the ability to stay his order or opinion, subject to FISCR review, but absent such an order by the judge, the opinion or order on the substantive surveillance matter should be effective immediately. This idea draws from concepts found in the ordinary course of appellate review of administrative action where appellate review is only available after an administrative action is "final."[70] In fact, under the Administrative Procedure Act, "final agency action" is a prerequisite to most causes of action.[71]

Again, an analogy to administrative law practice can help to make clear how the reviewability here would function. Consider what the Supreme Court held in *Bennett v. Spear*:

---

66. Note, *Constitutional Rights of Servicemen Before Courts-Martial*, 64 COLUM. L. REV. 127, 136 (1964).

67. *Id.*

68. Salve Regina Coll. v. Russell, 499 U.S. 225, 232 (1991) (citations omitted).

69. *Id.* at 231.

70. Bell v. New Jersey, 461 U.S. 773, 778 (1983).

71. *See* 5 U.S.C. § 704 (2012); Lujan v. Nat'l Wildlife Fed'n, 497 U.S. 871, 882 (1990).

> As a general matter, two conditions must be satisfied for agency action to be "final": First, the action must mark the "consummation" of the agency's decisionmaking process—it must not be of a merely tentative or interlocutory nature. And second, the action must be one by which "rights or obligations have been determined," or from which "legal consequences will flow."[72]

This essay's proposal of automatic appellate review upon issuing of an opinion or order satisfies the finality standard of *Bennett* in that once the FISC authorizes a surveillance activity, the agency is free to act on the opinion or order, and legal consequences clearly flow from actions on that opinion or order. The only issue raised by this essay's proposed process is that the opinion or order has the effects of a final order, but is not in fact finalized until the FISCR completes its review.

VII. PRESUMPTIVE PUBLICATION OF OPINIONS

With regard to publication of opinions, this essay argues that all opinions and orders of the FISC should be presumptively published, subject to appropriate redactions, and such redactions may require non-publication of entire opinions. However, all redaction and non-publication decisions are, like the "significant legal interpretations" discussed above, subject to automatic appellate review. The rationale supporting this presumption of publication is, in part, the same as that which supports the presumptive publication of "significant legal interpretations," specifically, judges who know their opinions are going to be reviewed will write those opinions in a way that is intended to survive judicial review. Second, by statutorily presuming that opinions are to be published, subject to appropriate redactions, the FISCR is now placed in the position of seeking ways to publish opinions, making only those redactions that are necessary to protect national security.

This is admittedly a more difficult task for the FISCR than the task of reviewing orders and opinions. Consider what David Kris and J. Douglas Wilson have written with regard to disclosure of FISA related information to the Judiciary Committees:

---

72. Bennett v. Spear, 520 U.S. 154, 177–78 (1997) (internal citations omitted).

> Some of the most significant legal issues under FISA arise at the intersection of (old) law and (new) technology, and FISA applications must discuss such issues if the Intelligence Community develops a new classified source or method of acquiring information that is subject to FISA. To take a fanciful case for purposes of illustration, imagine that the National Security Agency develops a new device that can read minds from a distance, like a kind of mental boom microphone. Information concerning this device would surely be classified Top Secret and also designated as Sensitive Compartmented Information (SCI). Before NSA could deploy the device inside the United States, government lawyers would need to confront the question whether its use constitutes "electronic surveillance" under FISA. If, as seems likely, the lawyers concluded that such use is "electronic surveillance," they would file an application with the FISC explaining the new technology and proposing minimization procedures for its operation. A summary of that FISA application, or of the interpretation of FISA from within it, would be hard to create without revealing the existence of the device. Such a revelation, of course, could compromise the use of the device, as spies, terrorists, and ordinary persons who value their privacy would immediately don tin-foil hats as a countermeasure.[73]

As the mind reader versus tin-foil hat example above illustrates, publication of opinions may be impossible in some cases. But, as the steady flow of redacted opinions following the Snowden leaks has made clear, not all opinions and orders require presumptive non-publication. Thus, shifting the presumption in favor of publication will cause the FISC to write opinions in a way that will enable redaction by the FISC itself, or by the FISCR. Because the task of balancing transparency and a presumption of publication against national security will be so difficult, the FISCR should be required to provide the government an opportunity to be heard on the harm to national security that might flow from the publication of opinions.

---

73. DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 13:3 (2d ed. 2014) (footnotes omitted).

VIII. REASONS FOR CYNICISM

While this Essay has proposed congressional action that will prompt greater transparency, there are reasons beyond national security for cynicism regarding the prospects for reform. Just consider that in much of the discourse surrounding national security surveillance, commentators will frequently say that the NSA is doing some horrible thing, usually followed by some comment about the NSA as a lawless organization.[74] Unfortunately, such comments are focused on the symptom, not the underlying disease. The underlying disease is that Congress wants things to operate the way that they do; Congress wants the FISC and has incentives to maintain the status quo.[75]

Why does Congress want the FISC? Because it allows those elected representatives to push accountability off to someone else. If members of Congress are responsible for conducting oversight of secret operations, their reputations are on the line if the operations go too far toward violating civil liberties, or not far enough toward protecting national security. However, with the FISC conducting operations, Congress has the ability to dodge accountability by claiming they have empowered a court to conduct oversight.

When that court gets things wrong, perhaps tightening the controls over surveillance in a way that allows threats to go undetected, elected officials can claim it was not their fault because the FISC would not let them do more. Similarly, when the court goes too far, enabling too much collection, rarely will the public hear about it. And, if the public does find out about it through leaks like Snowden's, government officials can claim the surveillance was in the interests of security, and that the activities were authorized by the courts. In both circumstances it allows elected officials to dodge political accountability. This highlights the challenge of democratic accountability in matters

---

74. *See, e.g.*, John Cary Sims, *What NSA Is Doing . . . And Why It's Illegal*, 33 HASTINGS CONST. L.Q. 105 (2006) (arguing that the surveillance program is illegal); G. Alex Sinha, *NSA Surveillance Since 9/11 and the Human Right to Privacy*, 59 LOY. L. REV. 861 (2013) (arguing that the surveillance program violates the human right to privacy).

75. For a discussion of the status quo bias generally, see Gregory S. McNeal, *The Status Quo Bias and Counterterrorism Detention*, 101 J. CRIM. L. & CRIMINOLOGY 855 (2011).

of national security — the problem is a mixed one: the FISC is not transparent about its decisions, but Congress lacks incentives to create transparency.

IX. CONCLUSION

The legal foundation for the section 702 program was widely debated in Congress. Members of Congress, advocacy groups, and the public were aware (or at least had the opportunity to make themselves aware) of the scope of the program which was based in large part on the Terrorist Surveillance Program. In contrast, the section 215 program relied upon a broad interpretation of a statute, that interpretation was argued in secret, issued in secret, not subject to appellate review, and not-disclosed to members of Congress while they were debating whether the statute enabling the section 215 program should be renewed. This interpretive secrecy and lack of democratic transparency is a significant failure of the FISA Court system.

The government cannot be faulted for following the system that was put into place by Congress, but the system is nevertheless faulty. Congress created a structure whereby the government can argue in an ex parte proceeding for an expansive interpretation of a statute, the initial application will only be reviewed by one judge, and that judge can issue an order in secret, without fearing appellate review or public rebuke. That system is destined to fail because it lacks democratic accountability. It is also suboptimal as it is bound to create poorly reasoned judgments and opinions.

In light of these problems, this essay argues that all FISC orders and opinions which rely upon or create a significant legal construction or interpretation should be subject to automatic de novo review by the FISCR. Second, all FISC orders and opinions should be presumptively public, subject to appropriate redactions, such redactions are automatically subject to de novo review by the FISCR. These two proposals will enhance the accountability of the FISC, will promote transparency, and will ensure better outcomes.