Washington and Lee Law Review

Volume 72 | Issue 3 Article 9

Summer 6-1-2015

Banning Bulk: Passage of the USA FREEDOM Act and Ending Bulk Collection

Bart Forsyth

Banning Bulk: Passage of the USA FREEDOM Act and Ending Bulk Collection

Bart Forsyth*

Table of Contents

* Bart is currently serving as chief of staff to Congressman F. James Sensenbrenner. He has also served as counsel to four other House committees—the Foreign Affairs Committee, the Science and Technology Committee, the Judiciary Committee, and the Select Committee on Energy Independence and Global Warming. On the latter of which, he was also the chief of staff. Bart played an active staff role in the drafting, introduction, and negotiation for House passage of the USA FREEDOM Act. The views in this Article are entirely his own and in no way reflect the views of any Member of Congress or Congressional Committee. Special thanks to all the Members and staff who helped shape and pass the USA FREEDOM Act, in particular, Caroline Lynch, Jason Herring, Aaron Hiller, Heather Sawyer, Lara Flint, Chan Park, Matt Owen, and Mike Lemon. Without their dedicated work, not only would this Article not be possible, neither would the law itself.

I. Introduction

When *The Guardian* published the initial Snowden revelations,[1] Congressman Jim Sensenbrenner's[2] reaction was immediate. He was the Chairman of the Judiciary Committee during the September 11 attacks and had negotiated the Patriot Act with the Bush Administration.

I was the Congressman's chief of staff. When Mr. Sensenbrenner announced his intent to introduce legislation to reverse what he saw as National Security Agency (NSA) overreach, I was tasked with spearheading his legislative response. These efforts led to the USA FREEDOM Act—a bill that would see several versions as it navigated the legislative process.[3]

While Foreign Intelligence Surveillance Act (FISA) reform and passage of the USA FREEDOM Act were ultimately political decisions, the Snowden leaks exposed several questions previously classified as legal in nature. This Article discusses a few of those

---

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 (last visited June 22, 2015) (on file with the Washington and Lee Law Review).

2. *See Biography*, CONGRESSMAN JIM SENSENBRENNER, http://sensenbrenner.house.gov/biography/ (last visited June 22, 2015)

> F. James Sensenbrenner, Jr., (Jim), represents the Fifth Congressional District of Wisconsin. The Fifth District includes parts of Milwaukee, Dodge and Waukesha counties, and all of Washington and Jefferson counties . . . . Shortly after the attacks of September 11, Jim introduced the PATRIOT Act in the House as a method to help keep America safe by enhancing the tools our law enforcement officials could use to thwart another terrorist attack. He was proud to watch President Bush sign the Act into law. Following revelations of the National Security Agency's bulk collection of data and the misinterpretation of Section 215 of the Patriot Act, Jim authored the USA FREEDOM Act—bipartisan, bicameral, and comprehensive legislation to rein in abuse, put an end to bulk collection, increase the transparency of the Foreign Intelligence Surveillance Court and ensure the proper balance between national security and privacy is struck.

(on file with the Washington and Lee Law Review).

3. *See Summary*: *H.R.3361—USA FREEDOM Act*, CONGRESS.GOV, https://www.congress.gov/bill/113th-congress/house-bill/3361 (last visited June 22, 2015) (showing an original version) (on file with the Washington and Lee Law Review).

questions and attempts to provide a brief overview of reform efforts.

Part II of this Article discusses the standard of production for tangible things under § 501 of FISA and the government's overbroad interpretation of that standard. Part III discusses the doctrine of judicial ratification in the context of legislation related to national security and argues that, in general, it should not apply. Part IV discusses legislative responses to the Snowden leaks and passage of the USA FREEDOM Act. Finally, Part V evaluates how the USA FREEDOM Act ends bulk collection.

II. Relevance Under Section 215

First and foremost, the USA FREEDOM Act reformed what Congressman Sensenbrenner believed was an overbroad interpretation of § 501 of FISA.[4]

The first leaked Snowden document was an order from the Foreign Intelligence Surveillance Court (FISC) directing Verizon to produce, on "an ongoing daily basis," all call detail records—primarily who called whom and how long they talked—of every call to or from every American, made either to, from, or within the United States.[5] Subsequent leaks confirmed that similar orders were issued to other major carriers.[6]

---

4. *See* Jim Sensenbrenner, *Abuse of the PATRIOT Act Must End*, THE GUARDIAN (June 9, 2013), http://www.theguardian.com/commentisfree/2013/jun/09/abuse-patriot-act-must-end (last visited June 22, 2015) ("The administration claims authority to sift through details of our private lives because the Patriot Act says that it can. I disagree. I authored the Patriot Act, and this is an abuse of that law.") (on file with the Washington and Lee Law Review).

5. Secondary Order at 1–2, *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc., No. BR 13-80 (Foreign Intelligence Surveillance Court Apr. 25, 2013), https://epic.org/privacy/nsa/Section-215-Order-to-Verizon.pdf [hereinafter Verizon Order].

6. *See* Dave Kravets, *Why AT&T's Surveillance Report Omits 80 Million NSA Targets*, WIRED (Feb. 21, 2014), http://www.wired.com/2014/02/ma-bell-non-transparency/ (last visited June 22, 2015) ("AT&T this week released for the first time in the phone company's 140-year history a rough accounting of how often the U.S. government secretly demands records on telephone customers.") (on file with the Washington and Lee Law Review).

The court granted the order under § 501 of FISA, the so-called business records provision.[7] Prior to passage of USA FREEDOM, § 501 allowed the Federal Bureau of Investigations (FBI) to obtain tangible things when, among other requirements, there were "reasonable grounds to believe that the tangible things sought [were] relevant to an authorized investigation."[8]

The major legal flaws were two-fold: first, the requirement for ongoing production was philosophically at odds with the purpose of § 501, in that it was seeking to obtain phone records on an ongoing prospective basis; second, the production of all records did not square with § 501's requirement that records be "relevant" to an authorized investigation.[9] Relevance is not a high legal standard, but in crafting § 501, Congress had contemplated a targeted authority that the government could use to obtain specific data.

How could everything be relevant? And if everything was relevant, what were the practical constraints of § 501?

There are, of course, instances when the government must—for investigative purposes—obtain a broader set of documents than just those that are ultimately critical to the investigation. In the government's words, "'[R]elevance' is a broad standard that permits discovery of large volumes of data in circumstances where doing so is necessary to identify much smaller amounts of information within that data that directly bears on the matter being investigated."[10]

---

7. Verizon Order, *supra* note 5, at 1.

8. 50 U.S.C. § 1861(b)(2)(A) (2012).

9. 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 (Jan. 23, 2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf; Jennifer Stisa Granick & Christopher Jon Sprigman, *The Criminal N.S.A.*, N.Y. TIMES (June 27, 2013), http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html (last visited June 22, 2015) (on file with the Washington and Lee Law Review).

10. ADMINISTRATION WHITE PAPER, BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 2 (2013), https://info.publicintelligence.net/DoJ-NSABulkCollection.pdf [hereinafter WHITE PAPER].

While this statement is overbroad,[11] it does describe how the government may need to collect a certain volume of records for investigative purposes. Imagine, for example, that the FBI determines an international terrorist purchased fertilizer to build a bomb from a farm store in Lexington, Virginia. Because the FBI does not know who the suspect is, all fertilizer sales made in Lexington, Virginia over a reasonable time period may well be relevant to the investigation—at least until the FBI determines which sale was actually made to the suspect.

In this way, the relevance standard can allow for a certain amount of bulk in a given collection. After the Snowden leaks, the government released a White Paper detailing its legal defense of the bulk collection of telephony metadata.[12] The government contends that, because communications metadata is interconnected, and because the connections between data points can only be analyzed from a large volume of data, the entire dataset is therefore relevant.[13]

In other words, for the government, all of our phone calls are like the fertilizer sales in Lexington, Virginia. Because the entire universe of America's phone calls undoubtedly contains some calls that are relevant to an authorized investigation, and because the government does not know which calls are of interest, that entire universe of calls is therefore relevant.

So how is the fertilizer example different from the government's collection of every phone call made by every American?

First, in the fertilizer hypothetical, there are stipulated facts that differentiate relevant fertilizer sales records from those that are not relevant to the investigation. Section 501 expressly calls for this by requiring, not that tangible things sought be relevant to an authorized investigation, but that the government produce a

---

11. As discussed below, the statement's underlying logic leads directly to bulk collection. If the government can collect large amounts of data when doing so is necessary to identify smaller amounts of data, then it can collect any broad record set on the assumption that individual pieces will contain information of interest.

12. *See* WHITE PAPER, *supra* note 10, at 2 (stating metadata collection was both statutorily authorized and constitutional).

13. *Id.*

"statement of facts showing" that the tangible things sought are relevant.[14] If this required statement of facts means anything, it must require that the statement of facts differentiate the relevant materials sought from the universe of all similar records.

In our hypothetical, the government is not simply requiring that every retailer produce all of its sales records. It is bringing forward facts that show it has reason to investigate fertilizer sales from a particular geographic location. The statement of facts is therefore separating the relevant documents from the entire universe of similar documents.

The only alternative would be that the statement of facts merely describes why the government needs the records. Under this rationale, § 501 would allow the government to collect any and all tangible things it deemed useful to an authorized investigation. If this was Congress's intent, it would have said as much.

With the bulk collection of telephony metadata, the government's statement of facts merely articulates a supposed value in collecting data on every call. There are no facts to differentiate calls that are more likely to relate to the government's investigation from every other call made by innocent Americans.

This leads to the second distinction between the fertilizer hypothetical and bulk metadata collection—the scope of the collection. The government's interpretation of the section is so broad that it ultimately conflates relevance with utility—the records are relevant because the government believes it needs them. This is not a standard at all.

Returning to—and distilling—the government's description of relevance: "'[R]elevance' is a broad standard that permits discovery of large volumes of data . . . where . . . necessary to identify much smaller amounts of information . . . ."[15] While this describes our fertilizer hypothetical, it also allows for any collection, no matter

---

14. *See* 50 U.S.C. § 1861(b)(2)(A) (2012)

> [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) conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities . . . .

15. WHITE PAPER, *supra* note 10, at 2.

how large, that includes at least some relevant data. The government's interpretation actually creates a perverse incentive to over-collect records because a larger volume of data is more likely to include relevant material.

In its White Paper, the government does attempt to articulate limits on what it can collect under § 501.[16] The government contends that the interconnectivity of phone metadata is what differentiates it from other types of tangible things.[17] Because one individual's phone metadata links to others' phone metadata, the information can be assembled into a singular web. Medical records, for example, are discrete, not interlocking, and therefore, an order for "all medical records" would not comport with the government's interpretation of § 501.[18]

The "interconnectivity" of records, however, does not differentiate relevant records from the broader universe of records—it simply distinguishes between different types of record sets. An awful lot of records would comport with the government's rationale. Emails, texts, sales transactions—who bought what from whom—who has visited what doctor and when, and essentially any other record that documented any form of social interaction could be assembled into a similar "web" and, therefore, could meet the government's definition of relevance.

Why interconnectivity should confer relevance is ultimately unclear—especially given that the government is not actually collecting a "web" of data. No such web exists. The phone companies never link these records into a web of data to create a single tangible thing. The government is simply collecting billions of individual records that, by its own admission, it has no legal basis to collect. The fact that the government eventually compiles all of these records into a database and performs a contact chaining process that could identify relevant records does not somehow retroactively add relevance to the documents, which of course, must be relevant at the time of collection.

---

16. *See id.* at 3 (noting that the Government can only collect information for counterterrorism purposes and cannot collect content of call or personal information).

17. *Id.* at 14.

18. *Id.*

Thus, interconnectivity confers relevance only if you confuse utility with relevance. None of this holds up to scrutiny under analysis of relevance, and there is little colorable suggestion that Congress intended to authorize this program. Neither the government nor the FISC seriously suggests otherwise.

In *ACLU v. Clapper*,[19] the Second Circuit agreed that the phone records of every American are not relevant under § 501.[20] The court equated § 501's standard to a grand jury subpoena.[21] While it acknowledged that the relevance standard used for a grand jury subpoena is broad, it is not limitless, and it must be tailored to fit a particular investigation.[22] The NSA's bulk collection program, by contrast, had no such limits. The court wrote, "[T]he records demanded are all-encompassing; the government does not even suggest that all of the records sought, or even necessarily any of them, are relevant to any specific defined inquiry."[23] As a result, the Second Circuit ruled that the government's bulk collection program violated the § 501 relevance standard.

Even though the USA FREEDOM Act amends § 501 to end bulk collection, the relevance standard remains in place in both § 501 and in other legal authorities. It therefore remains important to confront the government's overbroad approach.

To that end, the Second Circuit's decision in *Clapper* is welcome jurisprudence. In discussing relevance, future courts should consider an analytic framework that expressly examines (1) whether the government's theory of relevance differentiates the documents needed for its investigation from the broader universe of similar records to the greatest extent practicable, and (2) whether the government's theory of relevance is so broad that it ultimately conflates relevance and utility. This allows the government investigatory leeway without inappropriately opening all records to government collection.

---

19. 785 F.3d 787 (2015).

20. *See id.* at 812 ("We agree with appellants that such an expansive concept of 'relevance' is unprecedented and unwarranted.").

21. *See id.* at 811 ("Both the language of the statue and the legislative history support the grand jury analogy.").

22. *Id.* at 812.

23. *Id.*

The government seems to acknowledge that its interpretation of relevance is at best strained.[24] It therefore attempts to augment its interpretation of § 215 by arguing that Congress reauthorized the program after the government started its bulk collection program. The government writes, "It is significant to the legal analysis of the statute that Congress was on notice of this activity and of the source of its legal authority when the statute was reauthorized."[25] As discussed in the next section, this argument is also without merit.

III. Judicial Ratification of Classified Decisions

The government, the FISC, and at least one federal court have argued that, because Congress reauthorized § 501 after the FISC approved the bulk metadata collection program under the authority, Congress tacitly signaled its intent to enact the Administration's interpretation of the law.[26]

The Administration argued, "It is significant to the legal analysis of the statute that Congress was on notice of this activity and of the source of its legal authority when the state was reauthorized."[27] The basic premise is a well-established rule of judicial construction—known as ratification—that helps courts determine congressional intent by assuming Congress is aware of a public understanding of a law or phrase.[28] "Congress is presumed to be aware of an administrative or judicial interpretation of a

---

24. WHITE PAPER, *supra* note 10, at 17.

25. *Id.* at 2.

26. *See* Verizon Order, *supra* note 5, at 1 (ordering production of telephone metadata under 50 U.S.C. § 1861); WHITE PAPER, *supra* note 10, at 17–18 ("After receiving the classified briefing papers, which were expressly designed to inform Congress' deliberations on reauthorization of Section 215, Congress twice reauthorized this statutory provision, in 2010 and again in 2011."); ACLU v. Clapper, 959 F. Supp. 2d 724, 745 (S.D.N.Y. 2013) ("And viewing all the circumstances presented here in the national security context, this Court finds that Congress ratified section 215 as interpreted by the Executive Branch and the FISC, when it reauthorized FISA.").

27. WHITE PAPER, *supra* note 10, at 2.

28. *See* Bruesewitz v. Wyeth, LLC, 562 U.S. 223, 243 (2011) ("The consistent gloss represents the *public* understanding of the term." (emphasis added)).

statute and to adopt that interpretation when it reenacts a statute without change."[29]

This assumption is highly problematic when applied to legislation relating to national security, however, precisely because the judicial and administrative interpretations are not public. It is, therefore, much more difficult to know whether members of Congress actually know about a relevant interpretation of a law. As a result, courts should rarely, if ever, find that Congress ratified a classified statutory interpretation.[30]

The FISC first authorized the government's bulk collection of telephony metadata under § 501 in 2006.[31] In 2010 and 2011, Congress reauthorized § 501 without making any changes to the text.[32] In the interim, the Administration had made its interpretation of § 501 available to Congress.[33]

On a semiannual basis, the executive branch must provide reports to the House Permanent Select Committee on Intelligence (House Intelligence Committee or HPSCI), the Senate Select Committee on Intelligence (Senate Intelligence Committee or SSCI), and the House and Senate Judiciary Committees.[34] The reports must include (1) a summary of significant legal interpretations of § 501 involving matters before the FISC, and (2) copies of all decisions, orders, and opinions of the FISC that include a significant construction or interpretation of § 501.[35] The congressional reports are classified and are not made public.[36]

In addition to providing these classified reports to the Judiciary and Intelligence Committees, prior to the 2010 reauthorization, the executive branch made available to Congress "a classified, five-page document discussing the bulk telephony metadata program."[37] That classified document, which the

29. Lorillard v. Pons, 434 U.S. 575, 580 (1978).

30. The fact that classified legal interpretations are themselves problematic is outside the scope of this Article.

31. WHITE PAPER, *supra* note 10, at 1.

32. *Id.* at 18.

33. *Id.* at 17–18.

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

35. 50 U.S.C. § 1871 (2012).

36. *Id.*

37. *Clapper*, 959 F. Supp. 2d at 744.

government recently declassified in part, stated that "Section 501 orders generally require the production of the business records . . . relating to substantially all the telephone calls handled by the [telecommunication] companies, including both calls made between the United States and a foreign country and calls made entirely within the United States."[38]

Senate Intelligence Chairwoman Dianne Feinstein sent a letter to colleagues informing them that the Administration had made available a classified paper on "intelligence collection made possible by authority that is subject to the approaching sunset."[39] And House Intelligence Chairman Silvestre Reyes sent a letter informing his colleagues that "it is important that all Members of Congress have access to information about this program."[40]

Because of these disclosures, the government has argued, and the FISC and Judge Pauley in the U.S. District Court for the Southern District of New York have accepted, that Congress ratified the government's interpretation of § 501.[41] Judge Pauley wrote, "[V]iewing all the circumstances presented here in the national security context, this Court finds that Congress ratified section [501] as interpreted by the Executive Branch and the FISC, when it reauthorized FISA."[42] And writing for the FISC, Judge Claire Eagan found that "[t]he record before this Court thus demonstrates that the factual basis for applying the reenactment doctrine and presuming that in 2011 Congress intended to ratify Section 501 as applied by this Court is well supported."[43]

---

38. *Id.* at 745.

39. *Id.*

40. *Id.*

41. *See* WHITE PAPER, *supra* note 10, at 17–19 ("But to the extent there is any question as to the program's compliance with the statute, it is significant that, after information concerning the telephony metadata collection program carried out under the authority of Section 215 was made available to Members of Congress, Congress twice reauthorized Section 215."); Verizon Order, *supra* note 5, at 1 ("This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from Verizon Business Network Services, Inc. . . . satisfies the requirements of 50 U.S.C. § 1861."); ACLU v. Clapper, 959 F. Supp. 2d 724, 745 (S.D.N.Y. 2013) ("[T]his Court finds that Congress ratified section 215 as interpreted by the Executive Branch and the FISC, when it reauthorized FISA.").

42. *Clapper*, 959 F. Supp. 2d at 745.

43. Amended Memorandum Opinion at 27, *In re* Application of the Fed.

The concept of ratification fails, however, in highly classified settings because it depends entirely on a presumption of Congress's awareness about developments in the law. In a typical case, it is reasonable to assume that members of Congress are aware of a statutory interpretation prior to passing legislation. [44] This presumption is simply not reasonable in the national security context.

When information is classified, it is much more difficult for members to gain access to it. Reviewing classified material, even for a member of Congress, requires arranging time to travel to secure facilities to personally review information. A majority of members do not employ staff with sufficient clearances to review FISC decisions and other interpretations of national security authorities. In fact, staff in members' personal offices in the House of Representatives are not permitted to hold sufficiently high clearances, so most House members are not capable of employing cleared staff.

In a traditional area of law, there are almost countless ways for members to learn of judicial or administrative interpretations. There are press reports, email updates, Congressional Research Service memos, social media posts, phone calls from constituents and lobbyists, briefings from staff, casual conversations, and testimony at hearings. The interpretation is public and becomes a part of the legislative record and prep materials that members rely on. In this context, we know that members are aware of legal interpretations because they publicly discuss them.

The majority of these avenues are simply unavailable in the national security context. The result is that fewer members know about classified interpretations of statutes. How many fewer is impossible to know, and that is the crux of the problem in

---

Bureau of Investigation for an Order Requiring Prod. of Tangible Things From, No. BR 13-109 (Foreign Intelligence Surveillance Court Oct. 11, 2013), https://www.aclu.org/files/natsec/nsa/br13-09-primary-order.pdf.

44. *See* Forest Grove Sch. Dist. v. T.A., 557 U.S. 230, 239–40 (2009) ("Congress is presumed to be aware of an administrative or judicial interpretation of a statue and to adopt that interpretation when it re-enacts a statute without change."); Lorillard v. Pons, 434 U.S. 575, 580 (1978) (same); Bruesewitz v. Wyeth LLC, 562 U.S. 223, 243 (2011) ("When 'all (or nearly all) of the' relevant judicial decisions have given a term or concept a consistent judicial gloss, we presume Congress intended the term or concept to have that meaning when it incorporated it into a later-enacted statute.").

attempting to apply judicial ratification to classified interpretations of statutes. The logic underlying ratification—that it is reasonable to assume members knew about a judicial interpretation—does not apply.

In the case of § 501, Congress may have been actively misled by the Administration. Congressional oversight depends on honest testimony. At a hearing before the Senate Intelligence Committee, Senator Ron Wyden asked Director of National Intelligence James Clapper, "'Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?' Clapper responded, 'No, sir . . . not wittingly.'"[45]

While both the FISC and the district court in *Clapper* relied in part on ratification to uphold the government's bulk collection program, neither court was able to convincingly determine what members actually knew. Judge Pauley in *Clapper* posed the question regarding what members of Congress actually knew but ultimately concluded that it was enough that "the Executive Branch did what it was required to do under the statutory scheme that Congress put in place to keep Congress informed about foreign intelligence surveillance."[46] But no one accused the government of violating its disclosure laws. Judicial ratification is a matter of statutory interpretation, not a form of punishment for members of Congress perceived to have exercised insufficient due diligence.

In order for ratification to apply, the question should be: is it reasonable to assume that members of Congress were aware of a judicial and administrative interpretation and intended to adopt that interpretation into law? A finding that ratification does not apply in the national security context does not equate to a finding of wrongdoing in the executive branch. It is just an acknowledgement that the information is more difficult to come across and the logic underlying ratification is absent. Courts are poorly positioned to determine the extent to which members of Congress were aware of, and relied upon, classified information in the legislative process. As a result, judicial ratification should rarely, if ever, be applied to classified statutory interpretations.

---

45. Paul Campos, *How James Clapper Will Get Away with Perjury*, SALON (June 12, 2013), http://www.salon.com/2013/06/12/how_james_clapper_will_get_away_with_perjury/ (last visited June 23, 2015) (on file with the Washington and Lee Law Review).

46. *Clapper*, 959 F. Supp. 2d at 745.

In *Clapper*, the Second Circuit overturned Judge Pauley's ruling and rejected the government's argument that Congress ratified the Administration's determination. First, the court noted that ratification cannot overcome the plain meaning of a statute. "Where the law is plain, subsequent reenactment does not constitute an adoption of a previous administrative construction."[47]

The court further noted that the Supreme Court wrote in *Bruesewitz v. Wyeth LLC*, "The consistent gloss represents the *public* nature of the statutory interpretation is central to the doctrine."[48] The point is to help courts determine congressional intent. If a court does not know whether members were aware of a classified interpretation, it cannot logically assume that they intended to adopt it. In *Clapper*, the Second Circuit wrote,

> But here, far from the ordinarily publicly accessible judicial or administrative opinions that the presumption contemplates, no FISC opinions authorizing the program were made public prior to 2013—well after the two occasions of reauthorization upon which the government relies, and despite the fact that the FISC first authorized the program in 2006.[49]

Congress's response to the Snowden leaks confirms the logic underlying the Second Circuit's decision. Upon learning of the government's interpretation of § 501, members took concrete steps to block the changes. The nature of the debate was fundamentally different from previous debates to reauthorize the PATRIOT Act. Unlike previous reauthorizations, Congress openly discussed whether to allow bulk collection.[50]

---

47. ACLU v. Clapper, 785 F.3d 787, 819 (2d Cir. 2015) (quoting Demarest v. Manspeaker, 498 U.S. 184, 190 (1991)).

48. *Bruesewitz v. Wyeth*, 562 U.S. 223, 243 (2011) ("The consistent gloss represents the *public* understanding of the term." (emphasis added)).

49. *Clapper*, 785 F.3d at 820.

50. In a recent blog post, Professor Steven Vladeck touched upon this point:

> [G]iven what we *now* know about the government's interpretation of section 215, there'd be no way to view such a

It ultimately voted not to. Congress's rejection of bulk collection once the practice was public is strong evidence that it did not intend to ratify the Administration's classified interpretation. It is a lesson on the hazards of judging Congressional intent based on non-public information.

For the above reasons, courts should closely reexamine whether ratification makes sense in the context of national security decisions.

IV. The Procedural History of the USA FREEDOM Act

The Snowden leaks were public in June 2013.[51] Members and staff began work on the USA FREEDOM Act soon thereafter.[52] In July of that same year, Representative Justin Amash from Michigan introduced an amendment to the annual defense appropriation bill that *would* have stripped the NSA of funding for

---

> "clean" reauthorization as anything *other* than congressional ratification of that (dubious) reading of the statute—which would leave the Fourth Amendment challenge as the only remaining issue to be resolved by the Second, Ninth, and D.C. Circuits (and, perhaps, the Supreme Court). In other words, the closer we get to June 1 without meaningful discussion in Congress about section 215 reform, the more likely it is that we'll get a result that's *worse* than no reform–unqualified congressional validation of the government's deeply contested interpretation. That's not reform; that's entrenchment.

Steve Vladeck, *Whither the Section 215 Reauthorization Debate?*, JUST SECURITY (Mar. 19, 2015, 1:19 PM), http://justsecurity.org/21263/section-215-reauthorization-debate/ (last visited Aug. 10, 2015) (on file with the Washington and Lee Law Review).

51. *See* Mirren Gidda, *Edward Snowden and the NSA Files-Timeline*, THE GUARDIAN (Aug. 21, 2013, 5:54 PM), www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline (last visited May 10, 2015) (providing a timeline of the disclosures by Edward Snowden) (on file with the Washington and Lee Law Review).

52. *See* Chris Gentilviso, *Justin Amash's NSA Surveillance Amendment Ruled In Order*, HUFFINGTON POST (July 22, 2013, 11:34 PM), www.huffingtonpost.com/2013/07/22/justin-amash-nsa-surveillance_n_3637462.html (last updated July 23, 2013, 10:49 AM) (last visited May 10, 2015) ("A little more than a month after secret National Security Agency (NSA) surveillance programs were leaked to the public, one GOP congressman is making headway with his push to defund those initiatives.") (on file with the Washington and Lee Law Review).

its implementation of § 501.[53] Despite heavy lobbying against the amendment from House leadership of both parties and from the White House, the amendment was narrowly defeated by a vote of 217 to 205.[54]

The Amash amendment was a blunt, rather than a nuanced, response to the NSA overreach,[55] and it was aggressively opposed by both leadership and the White House.[56] Its narrow political defeat was thus a clear political signal that there was a strong desire for reform in the House of Representatives.[57]

This signal was augmented when Congressman Sensenbrenner introduced the USA FREEDOM Act that fall.[58] The bill attracted 152 cosponsors,[59] as well as the support of technology companies and privacy groups.[60] Importantly, twelve of the bill's cosponsors had voted against the Amash amendment—more than enough to have reversed the outcome of the vote.[61] In 2013, in the wake of the Snowden leaks, a clear majority of the House of Representatives favored reforming surveillance authorities.[62]

---

53. *See* Austin Wright, *Justin Amash Prevails as Amendment Fails*, POLITICO (July 24, 2013, 7:27 PM), www.politico.com/story/2013/07/justin-amash-nsa-amendment-94722.html (last updated July 27, 2013, 9:45 AM) (last visited May 10, 2015) (discussing the amendment Representative Amash introduced) (on file with the Washington and Lee Law Review).

54. *See id.* (discussing the Amash amendment).

55. *See id.* (describing the Amash amendment as a "controversial measure").

56. *See id.* ("The measure drew the ire of House Republican leaders and the White House.").

57. *See id.* (discussing how civil liberties advocates threatened to oppose any attempt to quash the amendment).

58. Dan Roberts, *Congressional Duo Launch NSA Overhaul Bill and Urge 'Meaningful Reform,'* THE GUARDIAN (Oct. 29, 2013, 12:51 PM), www.theguardian.com/world/2013/oct/29/nsa-overhaul-bill-legislation-usa-freedom-act (last visited May 10, 2015) (writing about the launch of the USA FREEDOM Act) (on file with the Washington and Lee Law Review).

59. *See* USA FREEDOM Act, H.R. 3361, 113th Cong. (1st Sess. 2013) (introducing the USA FREEDOM Act).

60. *See, e.g.*, *Open Letter to the Senate*, REFORM GOV'T SURVEILLANCE (May 19, 2015), www.reformgovernmentsurveillance.com/#111614 (last visited Aug. 20, 2015) (encouraging the Senate to pass the USA FREEDOM Act) (on file with the Washington and Lee Law Review).

61. *See* USA FREEDOM Act, *supra* note 59 (listing cosponsors of the USA FREEDOM Act).

62. *See* Wright, *supra* note 53 (discussing how the House of Representatives

While the depth of support was less clear in the Senate, Senator Patrick Leahy introduced an identical Senate companion bill.[63]

From the beginning, the surveillance debate exposed unusual Washington allegiances that were more about grassroots versus leadership than traditional partisanship.[64] Leadership from both parties and the White House opposed the bill upon its introduction,[65] but it was supported by some of the most liberal and conservative members of the House and Senate.[66]

Passing any legislation is difficult in the current political climate, but it is exponentially more difficult when the law in question is opposed by leadership.[67] Members supporting the bill, however, joined by outside privacy groups and tech companies, were putting near-constant pressure on Congress for reform.[68] In February 2014, a group of over forty technology companies and privacy groups organized an event titled "The Day We Fight Back" in an effort to encourage Congress to vote on the USA FREEDOM Act.[69] Congressman Sensenbrenner alone published eight op-eds

---

"overwhelmingly passed a separate NSA amendment . . . [that] would ensure the NSA [was] barred from acquiring or storing the content of emails and phone calls of people in the United States").

63. *See* USA FREEDOM Act, S. 2685, 113th Cong. (2d Sess. 2014) (introducing the identical Senate bill).

64. *See* Roberts, *supra* note 58 ("The measure also has more than 70 bipartisan co-sponsors in the House and enjoys the diverse support of groups ranging from the National Rifle Association to the American Civil Liberties Union.").

65. *See* Wright, *supra* note 53 (discussing opposition to earlier attempts to limit the NSA bulk-collection).

66. *See* Roberts, *supra* note 58 (listing members of both parties that supported the bill).

67. *See* Philip Bump, *The 113th Congress Is Historically Good at Not Passing Bills*, WASH. POST (July 9, 2014), www.washingtonpost.com/blogs/the-fix/wp/2014/07/09/the-113th-congress-is-historically-good-at-not-passing-bills (last visited May 10, 2015) (discussing Congress's inability to pass bills) (on file with the Washington and Lee Law Review).

68. *See supra* notes 59–60 and accompanying text (discussing the bipartisan support for the USA FREEDOM Act and the pressure from various groups).

69. *See* THE DAY WE FIGHT BACK, thedaywefightback.org (last updated Feb. 13, 2014) (last visited May 10, 2015) (calling on organizations and individuals to take action against mass surveillance) (on file with the Washington and Lee Law Review).

to help build momentum,[70] and there was a slow leak of disclosures from the Snowden documents, keeping the need for reform in the news.[71]

Senator Feinstein, the Chairwoman of the Senate Intelligence Committee, attempted to recapture the conversation by introducing the FISA Improvements Act.[72] The bill opened by stating its intent to end bulk collection, but then listed numerous exceptions that largely allowed the Administration to maintain the status quo.[73]

Senator Feinstein easily moved the FISA Improvements Act through her own committee, but the bill was poorly received outside the Intelligence Committee and was widely panned by

---

70. *See* Jim Sensenbrenner, *The Abuse of the PATRIOT Act Must End*, THE GUARDIAN (June 13, 2013, 7:00 PM), www.theguardian.com/commentisfree/2013/jun/09/abuse-patriot-act-must-end (last visited May 13, 2015) (discussing the Congressman's efforts to take action to curtail abuses of the Patriot Act) (on file with the Washington and Lee Law Review); Jim Sensenbrenner & Senator Pat Leahy, *The Case for NSA Reform*, POLITICO (Oct. 28, 2013, 9:40 PM), www.politico.com/story/2013/10/leahy-sensenbrenner-nsa-reform-98953.html (last updated Oct. 29, 2013, 6:42 AM) (last visited May 13, 2015) (calling for reform of the NSA) (on file with the Washington and Lee Law Review); Jim Sensenbrenner, *The NSA Overreach Poses a Serious Threat to Our Economy*, THE GUARDIAN (Nov. 20, 2013, 8:30 AM), www.theguardian.com/commentisfree/2013/nov/20/jim-sensenbrenner-nsa-over reach-hurts-business (last visited May 13, 2015) (same) (on file with the Washington and Lee Law Review); Jim Sensenbrenner, *NSA Abused Trust, Must Be Reined In*, MILWAUKEE J. SENTINEL (Nov. 2, 2013), www.jsonline.com/news/opinion/nsa-abused-trust-must-be-reined-in-b99131601z1-230292131.html (last visited May 13, 2015) (same) (on file with the Washington and Lee Law Review); Jim Sensenbrenner, *How Obama Has Abused the Patriot Act*, L.A. TIMES (Aug. 19, 2013), www.latimes.com/opinion/ op-ed/la-oe-sensenbrenner-data-patriot-act-obama-20130819-story.html (last visited May 13, 2015) (same) (on file with the Washington and Lee Law Review); Jim Sensenbrenner, *How Secrecy Erodes Democracy*, POLITICO (July 22, 2013, 11:12 PM), www.politico.com/story/2013/07/how-secrecy-erodes-democracy-94568.html (last visited May 13, 2015) (same) (on file with the Washington and Lee Law Review).

71. *See* Gidda, *supra* note 51 (citing to a timeline of the Snowden disclosures).

72. *See* FISA Improvements Act, S. 1631, 113th Congress (1st Sess. 2013) (introducing the FISA Improvements Act).

73. *See id.* (excepting a variety of bulk collection methods from the bill's scope).

editorial boards and outside groups.[74] It never received a vote on the Senate floor.[75]

Adding to the pressure for reform was that the business records provision, along with two other surveillance authorities from the PATRIOT Act—roving wiretaps and lone wolf—were set to sunset on June 1, 2015.[76] Increasingly, reform appeared to be the only way to save these authorities, and USA FREEDOM appeared to be the only acceptable vehicle for reform.[77]

Actual movement came when Chairman Mike Rogers of the House Intelligence Committee announced his intention to move his own FISA reform bill, The FISA Transparency and Modernization Act.[78] The bill was carefully structured, not only to maintain the status quo with regard to current surveillance programs, but to do so in a way that avoided triggering jurisdiction in the House Judiciary Committee.[79]

With its oversight of the judiciary and federal law enforcement, the Judiciary Committee was, historically, the primary committee of jurisdiction for surveillance authorities.[80]

---

74. *See, e.g.*, Nicole Ozer, *Sen. Dianne Feinstein's NSA 'Reforms': Bad for Privacy, Bad for Business*, AM. CIV. LIBERTIES UNION (Dec. 9, 2013, 2:29 PM), www.aclu.org/blog/national-security-technology-and-liberty/sen-dianne-feinsteins-nsa-reforms-bad-privacy-bad (last visited May 13, 2015) (criticizing the FISA Improvements Act) (on file with the Washington and Lee Law Review).

75. *See* FISA Improvements Act, *supra* note 72 (failing to go to a vote on the Senate floor).

76. *See, e.g.*, Nadia Kayyal, *Section 215 of the Patriot Act Expires in June. Is Congress Ready?*, ELEC. FRONTIER FOUND. (Jan. 29, 2015), www.eff.org/deeplinks/2015/01/section-215-patriot-act-expires-june-congress-ready (last visited May 30, 2015) (discussing the planned sunsetting of the roving wire taps and lone wolf provision) (on file with the Washington and Lee Law Review).

77. *See id.* (mentioning how the USA FREEDOM Act extended the sunset of § 215 by two years).

78. *See* The FISA Transparency and Modernization Act, H.R. 4291, 113th Cong. (2d Sess. 2014) ("Mr. Rogers . . . introduced the following bill.").

79. *See id.* (allowing for certain bulk collection programs and providing that "[t]he Foreign Intelligence Surveillance Court shall have jurisdiction to review").

80. *See* Spencer Ackerman, *NSA Critics Express "Deep Concern" Over Route Change for House Reform Bill*, THE GUARDIAN (Mar. 27, 2014, 7:35 AM), www.theguardian.com/world/2014/mar/26/nsa-critics-house-reform-bill-switch (last visited May 30, 2015) (discussing how review through the Intelligence Committee and not the Judiciary Committee was "highly unusual") (on file with

The HPSCI bill, therefore, was not only a dramatic substantive departure from USA FREEDOM, but also a significant jurisdictional shift.[81]

While nuanced, the issue of committee jurisdiction is significant.[82] Different committees and different committee chairs often have drastically different perspectives.[83] The Judiciary Committee is composed primarily of lawyers.[84] Their perspective is shaped by their legal backgrounds, as well as by their primary focus of overseeing federal law enforcement, such as the FBI, the Drug Enforcement Administration, and the other federal law enforcement entities.[85] Judiciary Committee members are typically well-versed in the Constitution and constitutional rights and view the government's interaction with the public through the prism of criminal law and its long history of regard for individual rights.[86]

The Intelligence Committee, by contrast, has primary jurisdiction over the Central Intelligence Agency and the NSA.[87] Its perspective is similarly shaped by these relationships, their

---

the Washington and Lee Law Review).

81. *See id.* (discussing the "deep concern" about the jurisdictional shift from the House Judiciary Committee to the Intelligence Committee).

82. *See id.* (discussing some of the ramifications of the jurisdictional shift).

83. *See* John R. Wright, *Contributions, Lobbying, and Committee Voting in the U.S. House of Representatives*, 84 AM. POL. SCI. REV. 417, 430 (1990) (providing an example of how the Ways and Means Committee consider themselves more senior, generally safer electorally, and concerned with broader and more important substantive problems than the Agricultural Committee).

84. *See About the Committee*, HOUSE COMMITTEE ON THE JUDICIARY, judiciary.house.gov/index.cfm/committee-members (last visited May 30, 2015) ("Due to the legal nature of the committee's work it has been customary for members of the committee to have a legal background.") (on file with the Washington and Lee Law Review).

85. *See id.* (listing the jurisdictional scope of the Judiciary Committee).

86. *See id.* (discussing the legal background and "breadth of knowledge" committee members often have, as well as the types of matters that come before the committee).

87. *See History and Jurisdiction*, H. INTELLIGENCE COMM. (last visited May 30, 2015) (discussing the jurisdiction of the Intelligence Committee) (on file with the Washington and Lee Law Review).

focus on clandestine activities, and the need to collect intelligence.[88]

A jurisdictional shift from the Judiciary to the Intelligence Committee could, therefore, have had a profound effect on the substance of our surveillance laws.[89] As a result, the Intelligence Committee Chair's decision to move the FISA Transparency and Modernization Act proved to be a critical motivator to convince House Judiciary Chairman, Bob Goodlatte, to move the USA FREEDOM Act.[90] The two committee chairs announced their intention to markup competing FISA reform bills on the same day.[91]

To avoid this conflict within the Republican Conference, then-House Majority Leader Eric Cantor organized a meeting with Chairmen Rogers, Goodlatte, and Sensenbrenner and asked that they reconcile the differences between their dramatically different bills.[92] Because a substantial majority of the House of Representatives favored reform, the USA FREEDOM Act became

---

88. *See id.* (discussing the oversight of the Intelligence Committee).

89. *See supra* notes 80–83 and accompanying text (discussing the impact of changing the jurisdiction to the Intelligence Committee from the Judiciary Committee).

90. *See, e.g.*, Dustin Volz, *House to Advance Bill to End Mass NSA Surveillance*, NAT'L J. (May 5, 2014), www.nationaljournal.com/tech/house-to-advance-bill-to-end-mass-nsa-surveillance-20140505 (last visited May 30, 2015) (discussing how the decision to hold a mark-up of the USA FREEDOM Act may have been "a counter to plans the House Intelligence Committee ha[d] to push forward a competing bill") (on file with the Washington and Lee Law Review).

91. *See id.* ("[J]ust hours after the Freedom Act earned a markup date, the Intelligence Committee announced it, too, would move forward with a markup of its own NSA bill—the FISA Transparency and Modernization Act.").

92. *See generally* Spencer Ackerman, *USA Freedom Act Unanimously Clears House Judiciary Committee*, THE GUARDIAN (May 7, 2014, 5:14 PM), www.theguardian.com/world/2014/may/07/usa-freedom-act-clears-house-committee-nsa-surveillance (last visited May 30, 2015) (discussing how the Intelligence Committee was also going to mark up the USA FREEDOM Act) (on file at Washington and Lee Law Review); Lisa Mascaro, *White House's Late Changes to NSA Spying Bill Shake Support*, L.A. TIMES (May 21, 2014, 7:28 PM), http://www.latimes.com/nation/politics/la-na-nsa-reforms-legislation-20140522-story.html (last visited Aug. 20, 2015) (discussing how "officials argued in the closed discussions" in House Majority Leader Eric Cantor's office and also discussing the changes to the USA FREEDOM Act) (on file with the Washington and Lee Law Review).

the basis for negotiations between the House Judiciary and Intelligence Committees.[93]

Prior to action, the two committees worked closely with the Administration and House leadership to review and negotiate the original bill.[94] The result was a significant narrowing of the text, though it still maintained its core functions of (1) ending bulk collection across all surveillance authorities, (2) increasing transparency and oversight of surveillance authority, and (3) reforming the FISC.[95]

The negotiated bill passed the Judiciary Committee unanimously on May 7, 2014.[96] The Intelligence Committee passed the identical text by voice vote.[97]

The period between committee and floor consideration led to another difficult round of negotiations with the Administration and House leadership.[98] Much of the difficulty stemmed from drafting technicalities, rather than substantive disagreements. On the one hand, proponents of reform believed that the government's expansive reading of relevance[99] necessitated a narrowly drafted ban on bulk collection.[100] The Administration, however, argued for broader construction because it worried that narrow language

---

93. *See* Ackerman, *supra* note 92 (discussing the support for the USA FREEDOM Act).

94. *See id.* (discussing the new version of the USA FREEDOM Act).

95. *See* USA FREEDOM Act, H.R. 3361, 113th Cong. (2d Sess. 2014) (presenting an edited version of the USA FREEDOM Act to the Senate). For a more detailed discussion of the USA FREEDOM Act, see *infra* Part V.

96. *See* Ackerman, *supra* note 92 (reporting the unanimous passing of the USA FREEDOM Act in the Judiciary Committee).

97. *See* Josh Gerstein & Alex Byers, *House Intel Surprises on NSA Surveillance*, POLITICO (May 8, 2014, 2:29 PM), www.politico.com/blogs/under-the-radar/2014/05/house-intel-surprises-on-nsa-surveillance-188205.html (last visited May 30, 2015) (discussing how the House Intelligence Committee passed the USA Freedom Act) (on file with the Washington and Lee Law Review).

98. *See* Julian Hattern & Christina Marcos, *House Votes 303-121 to Curb NSA*, THE HILL (May 22, 2014, 11:08 AM), thehill.com/policy/techynology/206929-house-votes-to-limit-nsa-spying (last visited May 30, 2015) (discussing the opposition the bill faced) (on file with the Washington and Lee Law Review).

99. *See supra* Part II (discussing the arguments surrounding the "relevance" wording).

100. Press Release, Rep. Zoe Lofgren., Rep. Zoe Lofgren Floor Statement on Opposing the USA FREEDOM Act (May 22, 2014) (on file with the author).

could be misinterpreted by the FISC to limit unintended collection.[101]

The result was compromise legislation that neither side thought perfect.[102] Importantly, the bill for the first time received the unqualified support of the White House. The White House endorsed the bill in an official policy statement that read:

> The bill ensures our intelligence and law enforcement professionals have the authorities they need to protect the Nation, while further ensuring that individuals' privacy is appropriately protected when these authorities are employed. Among other provisions, the bill prohibits bulk collection through the use of Section 215, FISA pen registers, and National Security Letters.[103]

Unfortunately, however, the bill lost the support of many of the key privacy groups and technology companies.[104] The primary objection was that the bill too narrowly defined the limiting term used to ban bulk collection.[105] Thus, while the USA FREEDOM Act easily passed the House of Representatives, it lost the support of some of its strongest congressional patrons.[106]

---

101. *See* David Kravets, *NSA Reform Falters as House Passes Gutted USA Freedom Act*, ARSTECHNICA (May 22, 2014, 1:12 PM), arstechnica.com/tech-policy/2014/05/nsa-reform-falters-as-house-passes-gutted-usa-freedom-act (last visited May 30, 2015) (discussing how the Obama administration pressured Republicans to water down the USA FREEDOM Act) (on file with the Washington and Lee Law Review).

102. *See id.* (providing views from different representatives about the watered down bill).

103. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY (2014).

104. *See* Andrea Peterson, *NSA Reform Bill Passes House Despite Loss of Civil Rights Groups*, WASH. POST (May 22, 2014), www.washington post.com/blogs/the-switch/wp/2014/05/22/nsa-reform-bill-passes-house-despite-loss-of-support-from-privacy-advocates/ (last visited May 30, 2015) ("But privacy advocates, technology companies and lawmakers warned that the version of the bill passed by the House was watered down to the point where they could no longer support it.") (on file with the Washington and Lee Law Review).

105. *See id.* (discussing how the initial version of the bill included a more narrow definition).

106. *Final Vote Results for Roll Call 230*, OFFICE OF THE CLERK (May 22, 2014), http://clerk.house.gov/evs/2014/roll230.xml (last visited August 4, 2015) (on file with the Washington and Lee Law Review).

In his statement on the House floor, Congressman Sensenbrenner conceded that the compromise legislation fell short in some respects, but nonetheless argued for the bill's support:

> Let me be clear, I wish this bill did more. To my colleagues who lament changes, I agree with you. To privacy groups who are upset about lost provisions, I share your disappointment. The negotiations for this bill were intense, and we had to make compromises, but this bill still deserves support. Don't let the perfect be the enemy of the good. Today, we have the opportunity to make a powerful statement: Congress does not support bulk collection.[107]

On May 22, 2014, the House of Representatives passed this version of the USA Freedom Act, with 303 votes in favor and 121 opposed.[108] Upon House passage, Senator Leahy put out the following statement:

> Today's action in the House continues the bipartisan effort to restore Americans' civil liberties. But I was disappointed that the legislation passed today does not include some of the meaningful reforms contained in the original USA FREEDOM Act. I will continue to push for these important reforms when the Senate Judiciary Committee considers the USA FREEDOM Act next month.[109]

Because so many privacy advocates and technology companies pulled their support for the House-passed version of the USA FREEDOM Act, Senator Leahy had the opportunity to reopen negotiations with the now-supportive Administration.[110] Senator

---

107. Press Release, Rep. F. James Sensenbrenner, Statement on the House Floor in Support of H.R. 3361 the USA FREEDOM Act (May 22, 2014) (on file with the author).

108. *See* Hattern & Marcos, *supra* note 98 (discussing the margin in which the House passed the USA FREEDOM Act).

109. Press Release, Sen. Pat Leahy, Comment of Senator Patrick Leahy (D-Vt.), Chairman, Senate Judiciary Committee, on House Passage of the USA FREEDOM Act (May 22, 2014) (on file with the author).

110. *See* Tom Risen, *Patrick Leahy Introduces Privacy Boosted USA FREEDOM Act*, U.S. NEWS (July 29, 2014, 12:07 PM), www.usnews.com/news/articles/2014/07/29/patrick-leahy-introduces-privacy-boosted-usa-freedom-act (last visited May 30, 2015) ("Leahy has been negotiating with the Obama administration and other members of the Senate and the intelligence community on changes to the legislation since a compromise version of the legislation passed the House.") (on file with the Washington and Lee Law Review).

Leahy succeeded in updating the House-passed legislation and rebuilding the bill's original coalition of privacy groups and technology companies, while maintaining support from the Administration.[111] Importantly, General James Clapper and Attorney General Eric Holder endorsed the bill, writing:

> The Intelligence Community believes that [the USA FREEDOM Act] preserves essential intelligence community capabilities; and the Department of Justice and the Office of the Director of National Intelligence support your bill and believe that it is a reasonable compromise that enhances privacy and civil liberties and increases transparency.[112]

Despite this coalition, the bill ultimately failed to meet the sixty-vote threshold for cloture in the Senate.[113] The USA FREEDOM Act thus died in the 113th Congress, despite support from 303 members of the House of Representatives and fifty-eight Senators.[114]

The Senate vote could have been the end of reform efforts.[115] Because, however, three surveillance provisions from the PATRIOT Act would sunset on June 1, 2015, there was a continued need to address privacy concerns stemming from government surveillance.[116] In early 2015, members began bipartisan,

---

111. *See* Kaylyn Groves, *Coalitions Support Leahy's USA FREEDOM Bill for Surveillance Reform*, ASS'N RESEARCH LIBRARIES (July 29, 2014), www.arl.org/news/arl-news/3332-coalition-supports-leahys-usea=freedom-bill-for-progress-toward-transparency-in-surveillance#.VWobvaPD9QU (last updated July 31, 2014) (last visited May 30, 2015) (discussing the groups that supported Leahy's version of the USA FREEDOM Act) (on file with the Washington and Lee Law Review).

112. Letter from Eric Holder, U.S. Attorney Gen., and James Clapper, Dir. Nat'l Intelligence, to Sen. Patrick Leahy, Chairman Sen. Judiciary Comm. (Sept. 2, 2014), http://fas.org/irp/news/2014/09/ag-dni-usaf.pdf.

113. *See* 160 CONG. REC. S6,075–03 (daily ed. Nov. 18. 2014) (roll call for Senator Leahy's USA FREEDOM Act garnering only fifty-eight yeas).

114. *See supra* notes 98, 113 and accompanying text (discussing the House and Senate votes on the USA FREEDOM Act).

115. *See* Adi Robertson & Nathan Ingraham, *USA Freedom Act for NSA Reform Is Voted Down in the Senate*, THE VERGE (Nov. 18, 2014, 8:29 PM), www.theverge.com/2014/11/18/7241967/usa-freedom-act-for-nsa-reform-is-voted-down-in-the-senate (last visited May 30, 2015) ("[N]ew legislation around this program will still be required despite the Senate's vote.") (on file with the Washington and Lee Law Review).

116. *See id.* (discussing the scheduled sunset of Section 215).

bicameral discussions to reconcile the House-passed version of the USA FREEDOM Act with the updated version introduced by Senator Leahy.[117]

On April 28, 2015, Congressmen Sensenbrenner, Goodlatte, Conyers, and Nadler reintroduced the USA FREEDOM Act.[118] The members had first reconciled the differences between the House and Senate versions of the bill with Senators Lee and Leahy, then with Chairman Devin Nunes, the new Chair of HPSCI, and finally with House leadership. Despite strong support in the House, Senate leadership had still not indicated support for the bill.

On May 13, the House of Representatives again passed the USA FREEDOM Act. The vote in 2015 was 338 in favor and eighty-eight opposed.[119] The overwhelming support was an important statement for the Senate.

With the sunset for the PATRIOT Act's surveillance authorities on the horizon, the Senate nonetheless dug in against the USA FREEDOM Act. Majority Leader Mitch McConnell, along with Senate Intelligence Chair Saxby Chambliss and Senate Judiciary Chair Chuck Grassley, pushed for a clean reauthorization of the PATRIOT Act authorities—an extension of the existing authorities without any reforms.[120] Meanwhile, Senator Rand Paul drew a hard line on the other side and advocated for a complete sunset of the authorities.

These tensions came to a head when Majority Leader McConnell brought the USA FREEDOM Act to the Senate floor on

---

117. *See* Spencer Ackerman, *NSA Reform Bill Imperiled as It Competes with Alternative Effort in the Senate*, THE GUARDIAN (Apr. 28, 2015, 9:03 PM), www.theguardian.com/us-news-2015/apr/28/house-nsa-reform-bill-senate-usa-freedom-act (last visited May 30, 2015) (discussing the 2015 USA FREEDOM Act version that was the product of ten weeks of "closed-door" negotiations in Congress) (on file with the Washington and Lee Law Review).

118. *H.R. 2048—USA FREEDOM Act of 2015*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/2048/actions (last visited Aug. 4, 2015) (on file with the Washington and Lee Law Review).

119. *Final Vote Results for Roll Call 224*, OFFICE OF THE CLERK (May 13, 2015), http://clerk.house.gov/evs/2015/roll224.xml (last visited Aug. 4, 2015) (on file with the Washington and Lee Law Review).

120. Kim Zetter, *Senate Fails to End NSA Bulk Spying, Votes Against USA FREEDOM Act*, WIRED (May 23, 2015), http://www.wired.com/2015/05/senate-fails-end-nsa-bulk-spying-votes-usa-freedom-act/ (last visited Aug. 4, 2015) (on file with the Washington and Lee Law Review).

May 22—just over a week before expiration of the PATRIOT Act authorities. Heavy lobbying from Senate hawks led to a narrow defeat on a procedural vote with fifty-seven Senators voting to proceed to debate on the USA FREEDOM Act, three votes short of the sixty-vote threshold for cloture.[121]

Senator McConnell attempted to pass a two-month reauthorization of the expiring authorities. The Senate, however, easily defeated his proposal. Senator McConnell then proposed a one-week extension, but Senator Paul objected, thereby blocking the vote.[122] McConnell suggested an extension until June 5, but Senator Wyden objected.[123] Then McConnell tried for June 3, only to have Senator Heinrich object.[124] Finally, the Majority Leader asked for an extension through June 2, but Senator Paul objected to even this twenty-four-hour extension of the expiring authorities.[125]

Exasperated, Majority Leader McConnell announced that the Senate would reconvene from its recess on May 31, just hours before expiration of the surveillance authorities. Late that night, the Senate voted 77–17 to proceed to consideration of USA FREEDOM.[126] Senator McConnell filed several amendments designed to weaken the civil liberties protections of the bill.[127]

---

121. Dustin Volz, Brendan Sasso, Sarah Mimms & Rachel Roubein, *How the Senate Fell Apart and Failed to Deal with the PATRIOT Act*, NAT'L J. (May 22, 2015), http://www.nationaljournal.com/tech/NSA-Patriot-Act-Rand-Paul-20150522 (last visited Aug. 20, 2015) (on file with the Washington and Lee Law Review).

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.*

126. Julian Hattem, *PATRIOT ACT Expires as Paul Blocks Final Vote on NSA Reform*, THE HILL (May 31, 2015), http://thehill.com/policy/national-security/243575-patriot-act-expires-as-paul-blocks-final-vote-on-NSA-reform. (last visited Aug. 20, 2015) (on file with the Washington and Lee Law Review).

127. *See* Robyn Greene, *Senators Should Oppose Senator McConnell's Amendments and Pass a Clean Version of the USA FREEDOM Act*, OPEN TECH. INST. (June 1, 2015), https://www.newamerica.org/oti/senators-should-oppose-senator-mcconnells-amendments-and-pass-a-clean-version-of-the-usa-freedom-act/ (last visited Aug. 4, 2015) (describing Senator McConnell's amendments to the USA FREEDOM Act; while McConnell initially offered more amendments, only three were ultimately brought to a vote) (on file with the Washington and Lee Law Review).

Senate rules, however, would not allow a vote on final passage of the bill or the amendments until Tuesday, June 2. As a result, three surveillance authorities from the USA PATRIOT Act temporarily sunset at 12:00 AM on June 1, 2015.

Any amendments to the House-passed bill would have, at the least, delayed reauthorization of the authorities, as the House of Representatives would have had to vote on the Senate-amended bill. There was also no guarantee that the House would accept the Senate's changes. As a result, Senator McConnell was bucked by his own party as the Senate voted down each of his amendments by a simple majority vote. The Senate then passed the identical language as the House, 67–32, enacting the USA FREEDOM Act into law.[128]

V. The USA FREEDOM Act's Ban on Bulk Collection

The USA FREEDOM Act was always intended to end bulk collection, but the way the bill met this goal evolved during the legislative process.[129]

Upon introduction, the USA FREEDOM Act sought to end bulk collection by crafting new standards of collection across government surveillance authorities.[130] When, however, the House Judiciary and Intelligence Committees scheduled the bill for markup, the FBI privately worried that the new standard could have unintended consequences for individual collection.[131]

To address this concern, members settled on a different approach whereby the standard for individual collection was left intact, but USA FREEDOM added a new requirement that the

---

128. *U.S. Senate Roll Call Votes 114th Congress – 1st Session*, SENATE.GOV (June 2, 2015), http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=114&session=1&vote=00201 (last visited Aug. 4, 2015) (on file with the Washington and Lee Law Review).

129. *See* FISA Improvements Act, S. 1631, 113th Cong. (1st Sess. 2013) (discussing the core function of the USA FREEDOM Act); *supra* Part IV (discussing the evolution of the USA FREEDOM Act).

130. *See* USA FREEDOM Act, H.R. 3361, 113th Cong. (1st Sess. 2013) (limiting the manner in which the government could collect data).

131. *See supra* notes 8–13 and accompanying text (discussing the allowances § 215 gives to the FBI).

government include a "specific selection term" as the basis for production under (1) § 501, (2) for orders for a pen register trap and trace device, and (3) for various national security letter (NSL) authorities.[132]

Section 501 of FISA

USA FREEDOM expands the § 501 surveillance authority with a specific new mechanism for the collection of call detail records.[133] The mechanism grew out of a proposal that President Obama proposed in January, 2014. The President announced reforms to the collection of signals intelligence by the federal government and issued Presidential Policy Directive (PPD). For collection of business records other than call detail records, the USA FREEDOM Act requires the government to use a specific selection term as the basis for production.

In January, 2014 the Administration released Presidential Policy Directive (PPD 28), which defined bulk collection as the acquisition "of large quantities of signals intelligence data which . . . is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)."[134] By requiring a specific selection term, the USA FREEDOM Act therefore, by definition, ended bulk collection.[135] But would this new limitation be sufficient in practice?

---

132. USA FREEDOM Act, H.R. 3361 § 103 (as reported by the House Judiciary Committee).

133. "Call detail records" include "session identifying information (including originating or terminating telephone number, International Mobile Subscriber Identity number, or International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call." USA FREEDOM Act, § 107, Pub. L. No. 114-23, § 107, 129 Stat. 268 (2015).

134. Presidential Policy Directive—Signals Intelligence, PPD-28, OFF. OF THE PRESS SECRETARY (Jan. 17, 2014), www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (last visited June 14, 2015) (on file with the Washington and Lee Law Review).

135. The definition of SST was easily the most heavily debated portion of the bill. *See* 160 CONG. REC. H4793,4801 (daily ed. May 22, 2014) (debating the definition of "specific selection term"). The definition saw several versions from the House-passed bill, to the Senate-introduced bill, to its reintroduction in the 114th Congress. *See id.* (discussing the different versions of the term while debating its meaning). The intent of the specific selection term and its role in ending bulk collection, however, remained constant across these bills. *See infra* note 141 (discussing the meaning of the term). The next portion of this Article

While virtually every line of the Act's text was subject to scrutiny and negotiation, there was no aspect of the bill that garnered more intense focus than the definition of specific selection term. It was primarily this definition that led many technology companies and privacy groups to pull their support for the USA FREEDOM Act after it first passed the House in 2014.[136] It was only after Senator Leahy redrafted the definition that these organizations again supported the bill.

In drafting the statute, it became clear that bulk collection—at least the bulk collection most members objected to—was less about the exact quantity of tangible things sought than the indiscriminate nature of the collection.[137] As discussed in Part II, this was the critical distinction between the government's metadata collection program and our fertilizer hypothetical.[138] The metadata collection program is considered "bulk," while the fertilizer hypothetical is not because the collection of fertilizer sales is no broader than necessary for the purpose of the investigation.[139]

The relevance standard should have required a statement of facts that separated the necessary documents or tangible things from the broader universe of similar tangible things, but the government interpreted the standard to obviate this analysis and ultimately conflate relevance and utility—the government believed it should have access to any data that could serve a useful investigatory purpose.

As enacted, the USA FREEDOM Act defines a specific selection term as:

---

discusses the SST in terms of this general intent, rather than the specifics of the different definitions.

136. H.L. Pohlman, *The NSA FREEDOM Act?*, WASH. POST (May 27, 2014), http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/05/27/the-nsa-freedom-act/ (last visited Aug. 20, 2015) (on file with the Washington and Lee Law Review).

137. *See* 160 CONG. REC. H4800 (daily ed. May 22, 2014) (statement of Rep. Dutch Ruppersberger) (discussing how bulk collection means the "indiscriminate acquisition of information").

138. *See supra* Part II (discussing the distinctions between metadata collection and the hypothetical presented).

139. *See* 160 CONG. REC. H4793–4801 (daily ed. May 22, 2014) (statement of Rep. Dutch Ruppersberger) (discussing metadata collection).

> (i) IN GENERAL - Except as provided in subparagraph (B), a 'specific selection term'—
>
> (I) is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and
>
> (II) is used to limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things.
>
> (ii) LIMITATION.—A specific selection term under clause (i) does not include an identifier that does not limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things, such as an identifier that—
>
> (I) identifies an electronic communication service provider (as that term is defined in section 701) or a provider of remote computing service (as that term is defined in section 2711 of title 18, United States Code), when not used as part of a specific identifier as described in clause (i), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used as the basis for the production; or
>
> (II) identifies a broad geographic region, including the United States, a city, a county, a State, a zip code, or an area code, when not used as part of a specific identifier as described in clause (i).[140]

The complexity of the definition reflects the intensity of negotiations over the term. A lot of the analysis of the definition focused on the initial clause and the limitation. The fact that a specific selection term cannot be used to identify an "electronic service provider" or a "broad geographic area" is an important restriction, but the key to the new legal standard is that the specific selection term must be "used to limit, to the greatest extent reasonably practicable, the volume of tangible things sought consistent with the purpose for seeking the tangible things."[141] The SST is, therefore, not intended to put a cap on the total amount of

---

140. USA FREEDOM Act, § 107, Pub. L. No. 114-23, § 107(k)(4)(A)(i)–(ii), 129 Stat. 268 (2015).

141. *Id.* § (k)(4)(A)(i)(II). This is the definition used in the most recent version of the USA FREEDOM Act, but the goal was consistent throughout beginning with the House-passed version of the USA FREEDOM Act and extended into the Senator Leahy's new Senate version. *See* 161 CONG. REC. S2772 (daily ed. May 12, 2015) (statement of Sen. Mike Lee) (discussing the meaning of "specific selection term" and why the term was included in the bill).

records, but instead, to limit the number of records to the greatest extent possible.[142]

As discussed in Part II, this limitation should have been considered an essential aspect of the relevance standard.[143] Because it was not, the USA FREEDOM Act explicitly codified the limitation. The standard requires a case-by-case, fact-specific determination by the FISC as to whether the government's request is limited to the "greatest extent reasonably practicable."[144]

> USA FREEDOM also expands the Section 501 surveillance authority with a specific new mechanism for the collection of call detail records.[145] The mechanism grew out of a policy that President Obama proposed in January, 2014. The President announced reforms to the collection of signals intelligence by the federal government and issued PPD 28.[146] He directed that the FISC would first approve queries of telephone metadata collected by the NSA under Section 501 of FISA and that such queries would be limited to two "hops."[147]

USA FREEDOM relies on these reforms and establishes a new, narrowly-tailored mechanism for the targeted collection of telephone metadata. It is narrower than the bulk program the government operated prior to PPD 28, but broader than what would otherwise be allowed under § 501 as amended by the USA FREEDOM Act.

If the government can demonstrate a reasonable, articulable suspicion that a specific selection term[148] is associated with a

---

142. *See id.* (discussing why Congress added the term to the USA FREEDOM Act).

143. *See id.* (discussing the problems with the relevance standard).

144. *See* USA FREEDOM Act, § 107(k)(4)(A)(i)(II) (codifying the specific selection term as a limitation to bulk collection).

145. *See supra* note 133 (defining call detail records).

146. Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

147. *Id*.

148. For the purposes of the call detail records program, a specific selection term is defined as "a term that specifically identifies an individual, account, or personal device." USA FREEDOM Act, § 107, Pub. L. No. 114-23. As discussed later in this section, the Act uses a different definition of specific selection term for the production of all other tangible things.

foreign power or an agent of a foreign power engaged in international terrorism, the FISC may issue an order for the ongoing, daily production of call detail records held by telephone companies. The FISC may order the production of up to two "hops"—i.e., the call detail records associated with the initial telephone number and the records associated with the records returned in the initial hop.[149]

This new authority—designed to allow the government to search telephone metadata for possible connections to international terrorism—does not preclude the government's use of standard business records orders under Section 501 to compel the production of business records, including call detail records, but the collection would not be prospective and the government likely could not collect "two hops" from the targeted individual.

VI. The USA FREEDOM Act's Ban on Bulk Collection Across Other Authorities

Section 201 of the Act prohibits bulk collection under the pen register and trap and trace device authority by requiring that each application include a specific selection term as the basis for the use of the device.

The definition of "specific selection term" is similar to the definition of that term for § 501 orders. Specifically, it is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier, that is used to limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for the use of a pen register or trap and trace device. It does not include terms that are not so limited, such as terms based on a broad geographic region or service provider.

Finally, § 501 of the USA FREEDOM Act prohibits the use of various NSL authorities (contained in the Electronic

149. A second "hop" does not include an individual listed in a telephone contact list, or on a personal device that uses the same wireless router as the seed, or that has similar calling patterns as the seed. Nor does it exist merely because a personal device has been in the proximity of another personal device. These types of information are not maintained by telecommunications carriers in the normal course of business and, regardless, are prohibited under the definition of "call detail records."

Communications Privacy Act, Right to Financial Privacy Act, and Fair Credit Reporting Act) without the use of a specific selection term as the basis for the NSL request. It specifies that for each NSL authority, the government must specifically identify the target or account.

VII. Conclusion

Negotiating FISA reform, I sometimes imagined my intelligence-minded colleagues looking with bewilderment at those of us across the table who were working to end bulk collection. Why exactly should we care?

It is a fair question. It would be a clean line if we believed that our records were somehow inviolable—that our records are our own and our right to keep them from the government is absolute, absent some suspicion of wrongdoing. But virtually all proponents of reform concede that this standard would be too restrictive for records not protected by the Fourth Amendment.[150] The government does, in some instances, need to collect "large volumes of data" to identify "smaller amounts of information" that bear on an investigation.[151]

So if the government can collect the records of innocent persons for investigative purposes in some circumstances, why can it not in others?

Ultimately, the limits are a check on government power.[152] Just as we are naïve to ignore the very real threats to our national security, we would be equally naïve to ignore the very real encroachments our government has made on civil liberties at

---

150. *See* Casey J. Mcgowan, Note, *The Relevance of Relevance: Section 215 of the USA Patriot Act and the NSA Medatata Collection Program*, 82 FORDHAM L. REV. 2399, 2439 (2014) (discussing middle ground where the NSA is not completely prevented from collecting data outside of the Fourth Amendment).

151. *See* WHITE PAPER, *supra* note 10, at 2.

152. *See* Dan Froomkin, *USA Freedom Act: Small Step for Post-Snowden Reform, Giant Leap for Congress,* THE INTERCEPT (June 2, 2015), firstlook.org/theintercept/2015/06/02/one-small-step-toward-post-snowden-surveillance-reform-one-giant-step-congress/ (last visited June 14, 2015) (discussing the limits the USA FREEDOM Act puts on the government's ability to bulk collect) (on file with the Washington and Lee Law Review).

perilous times in our country's history. Under the government's definition of relevance, the government can indiscriminately collect and store data when it believes the datasets are potentially valuable.[153] Once the FISC accepts this construct, the line becomes the government's to draw.

Limits on government power matter. Maybe more importantly, where those limits are drawn should be a political question. If the government is to conduct bulk collection—and the courts ultimately deem it constitutional—it should be a democratic choice made by elected officials accountable to the voters.

The USA FREEDOM Act represents a clear political product, drafted as an honest attempt to equip the intelligence community with the tools it needs without unnecessarily compromising privacy or civil liberties. There is no perfect place to draw the line between privacy and national security. The Constitution does, however, establish that the political process is the perfect way to draw it.

153. *See id.* (discussing how the government can still access metadata it deems to be relevant).