Santa Clara Law Review

Volume 55 | Number 1 Article 4

10-7-2015

The Freedom of Information Act and the Fight Against Secret (Surveillance) Law

Mark Rumold

THE FREEDOM OF INFORMATION ACT AND THE FIGHT AGAINST SECRET (SURVEILLANCE) LAW

Mark Rumold*

TABLE OF CONTENTS

INTRODUCTION

In June 2013 the disclosure of the now-infamous Verizon order—leaked by Edward Snowden and published by the *Guardian*—shocked the public. The order required disclosure to the NSA all records of domestic and international calls on Verizon Business Network Services—an order which swept in the call records of millions of Americans.[1] The order,

* Staff Attorney, Electronic Frontier Foundation.

1. *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, BR 13-80 FISC (July 19, 2013); Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013),

splashed across the pages of a British newspaper complete with its TOP SECRET markings, caused a tremendous public outcry. Rightfully, the public was taken aback by the order's sweeping breadth, the NSA's gathering of information on Americans, and, for many, the revelation that America had a secret surveillance court.

However, to those watching surveillance issues closely, the existence of the program was no secret. Indeed, details of the program were first published in *USA Today*, seven years before the *Guardian*'s story.[2] While the program's existence was not entirely secret, its legal basis was. And, with no public law that explicitly authorized such conduct, civil liberties advocates were left wondering: How could this be legal?[3] Nevertheless, aside from grumblings from a few members of Congress, the government had been able to stay remarkably silent about the ways it had interpreted Section 215, the provision of the Foreign Intelligence Surveillance Act it relied on to obtain call records in bulk.[4]

The public debate that followed the *Guardian*'s disclosure did not prove to be a ringing endorsement of that secret legal interpretation or the democratic processes that gave rise to it. Less than a year after the program's full public disclosure, the call records collection program appears to be on its last legs, both legally and politically. At least one court has declared it unconstitutional;[5] two separate, independent executive branch oversight bodies have recommended its end;[6] President Obama has signaled he intends to end the program;[7] and, after reviewing the program for only a few

---

http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

2. Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY (May 11, 2006), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

3. The short answer: it's not.

4. *See infra* at 5–11.

5. Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013).

6. PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD (2013); DAVID MEDINE ET AL., PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014).

7. Anita Kumar, *Obama Signals Changes Likely to NSA Spying*, MCCLATCHY WASHINGTON BUREAU (Dec. 20, 2013), http://www.mcclatchydc.com/welcome_page/?shf=/2013/12/20/212377_obama-

months, government officials were able to conceive of ways of achieving the call records collection program's objectives in a manner more sensitive to civil liberties.[8] For a program that, as the government touted, "all three branches of government" participated in, one would expect it could survive more than a year's worth of public scrutiny.[9]

The story of Section 215 serves as a cautionary tale for excluding the public from the debate on surveillance techniques and the interpretation of federal surveillance laws. But the problem of secret reinterpretation of surveillance laws is not one unique to Section 215. It is a problem that constantly recurs: as new surveillance technologies or programs emerge, government officials inevitably seek to press those techniques into service within already existing legal authorities. Because law enforcement officials are hesitant to disclose these techniques, and the legal analysis supporting them, for fear of disclosing surveillance "sources and methods," the public is left in the dark—both about the use of new techniques and the legal authority that supports it.[10]

This article proposes a modest solution for the problem of secret interpretations of surveillance law. The Freedom of Information Act (FOIA), with only a measured extension of current law and practice, is well-equipped to guard against precisely this problem. Using a stalwart of FOIA litigation, the *Vaughn* index, this Article argues that courts should and, indeed, are already empowered to compel the government to provide summaries of the legal rationale underlying otherwise-sensitive surveillance programs. This type of modified *Vaughn* index—a "tearline *Vaughn*"—could help bridge the current gap between the government's need to protect "sources and methods" and the democratic need for public accountability and legitimacy.

---

signals-changes-likely-to.html.

8. Statement of Administration Policy, OFFICE OF MGMT. & BUDGET (Nov. 17, 2014), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saps2685s20141117.pdf.

9. *See* Cheryl Pellerin, *Officials Discuss Intelligence Programs at Senate Hearing*, U.S. DEPARTMENT OF DEFENSE (Sept. 27, 2013), http://www.defense.gov/news/newsarticle.aspx?id=120873.

10. *See infra* Part II.A.

I. THE SECRET STORY OF SECTION 215

In a 2011 speech on the Senate floor, Senator Ron Wyden ominously declared:

> I have served on the Intelligence Committee for over a decade and I wish to deliver a warning this afternoon. When the American people find out how their government has secretly interpreted the PATRIOT Act, they are going to be stunned and they are going to be angry. . . . The fact is anyone can read the plain text of the PATRIOT Act. Yet many Members of Congress have no idea how the law is being secretly interpreted by the executive branch[.][11]

That day came on June 5, 2013, when, as described above, the *Guardian* published an order issued by the Foreign Intelligence Surveillance Court.[12] But the story of Section 215 and the NSA's bulk collection of Americans' call records began over a decade before.

Shortly after September 11, 2001, the NSA began collecting Americans' call records in bulk from two major telecommunication companies.[13] In the beginning of the program, there were no court orders; instead, the companies were provided with presidential "authorizations" that stated the Attorney General had determined the program to be legal.[14]

For nearly five years, the call records program continued in secret—alongside other NSA domestic surveillance programs— "justified" on the basis of the President's inherent executive authority alone.[15] In December 2005, NSA's domestic surveillance programs made their first public appearances. First, the *New York Times* reported that President Bush had authorized the NSA to spy within the

---

11. 157 CONG. REC. S3,386 (daily ed. May 26, 2011).

12. Greenwald, *supra* note 1.

13. OFFICE OF THE INSPECTOR GENERAL, ST-09-0002 WORKING DRAFT 33–34 (2009), *available at* http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection [hereinafter OIG WORKING DRAFT REPORT]. A third company began providing call detail records in December 2002.

14. OFFICES OF INSPECTORS GENERAL, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM (2009), *available at* www.fas.org/irp/eprint/psp.pdf; OIG WORKING DRAFT REPORT, *supra* note 13.

15. *Id*. at 39–40.

United States without warrants.[16] Then in May 2006, *USA Today* disclosed the call records program.[17] While President Bush and other government officials confirmed portions of the *Times*' account, the government managed to avoid confirming the accuracy of *USA Today's* story.[18]

While the disclosures did not change the government's legal approach, the firms participating in the program developed cold feet. Shortly after the *New York Times* disclosures, lawsuits were filed across the country against telecommunication companies, like AT&T and Verizon, alleging violations of federal wiretapping and privacy laws by assisting the government.[19] In light of these suits, and to put the disclosure of call records to the NSA on ostensibly firmer legal footing, the telcos requested that the call records program be shifted to a court-ordered regime.[20] By May 24, 2006—less than a month after the program's disclosure in *USA Today*—the Foreign Intelligence Surveillance Court (FISC) issued its first Section 215 order for the bulk collection of Americans' call records.[21]

The provision of law the government relied on, 50 U.S.C. § 1861, is commonly known as Section 215—taking its name from the provision of the USA PATRIOT Act of which it was a part. The Patriot Act amended the "business records" provision of the Foreign Intelligence Surveillance Act. Section 215 broadened what had previously been a narrow authority to obtain records of "common carriers," such as hotel records, car rental records, and storage unit rentals.[22] It authorized the FBI, upon an application to the Foreign Intelligence Surveillance Court, to compel the production of "any tangible thing[]" from a third-party that was "relevant" to an authorized foreign intelligence investigation.[23] It is this statutory language that was stretched to give the NSA, not

16. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, NEW YORK TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html.

17. Cauley, *supra* note 2.

18. *See id.*

19. *NSA Multi-District Litigation*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/cases/nsa-multi-district-litigation.

20. OFFICE OF THE INSPECTORS GENERAL, *supra* note 14.

21. *See id.*

22. 50 U.S.C. § 1862 (2006).

23. 50 U.S.C. § 1861(b)(2)(A) (2006).

the FBI, the authority to obtain past and future call record information on millions of Americans with no connection to terrorism or any other "authorized foreign intelligence investigation."[24]

Of course, the FISC's orders remained secret, and the program continued largely unchanged and uninterrupted. Although Department of Justice (DOJ) attorneys publicly disclosed that Section 215 orders were being used to support a "sensitive collection program" in 2009,[25] from 2006 to 2013, Section 215 was discussed only fleetingly in public, primarily in the context of Section 215's various reauthorizations.

In 2009, Senator Richard Durbin, a member of the Senate Judiciary Committee, stated that "the government's use of Section 215 is unfortunately cloaked in secrecy. Some day that cloak will be lifted, and future generations will ask whether our actions today meet the test of a democratic society: transparency, accountability, and fidelity to the rule of law and our Constitution."[26] Similarly, then-Senator Russ Feingold, a member of both the Senate Judiciary Committee and the Senate Select Committee on Intelligence ("SSCI"), stated: "There is information about the use of Section 215 orders that I believe Congress and the American people deserve to know . . . at least basic information about how they have been used."[27]

In May 2011, two Senators on the SSCI again voiced public concerns about the government's use of Section 215 orders. Senator Mark Udall echoed concerns, similar to his colleagues earlier concerns, about the scope of Section 215: "Congress is granting powers to the [E]xecutive [B]ranch that lead to abuse, and frankly, shield the [E]xecutive [B]ranch from accountability."[28] Two days later, Senator Udall argued that the executive's "official interpretation of" the nation's

---

24. *Id.* § 1861.

25. *Hearing on the USA Patriot Act Before the Subcomm. on Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111 Cong. 8 (2009) (testimony of Todd Hinnen).

26. *Executive Business Meeting* Before the Senate Committee on the Judiciary, 111 Cong. (2009) (Remarks of Sen. Richard Durbin) (Remarks begin at 68:00), *available at* http://www.judiciary.senate.gov/meetings/executive-business-meeting-2009-10-01.

27. 155 CONG. REC. S9,563 (daily ed. Sept. 17, 2009) (statement of Sen. Feingold).

28. 157 CONG. REC. S3258 (daily ed. May 24, 2011).

laws should not "be kept secret."[29] To that end, when Section 215 was scheduled to expire in 2011, Senators Wyden and Udall co-sponsored an amendment to its reauthorization, requiring government officials to "not secretly reinterpret public laws and statutes" and to "not describe the execution of these laws in a way that misinforms or misleads the public."[30]

In a September 2011 letter, Senators Wyden and Udall again criticized DOJ officials for making "misleading statements pertaining to the government's interpretation of surveillance laws."[31] The letter criticized DOJ's claims that Section 215 was being used in ways analogous to grand jury subpoenas, claims the Senators "consider[ed] highly misleading" and that "provide[d] the public with a false understanding of how surveillance law is interpreted in practice."[32] The letter also criticized DOJ's claims that Section 215 was not a "secret law;" as the letter noted, "when the government relies on significant interpretations of public statutes that are kept secret from the American public, the government is effectively relying on secret law."[33]

Finally, in March 2012, Senators Wyden and Udall wrote in a letter to Attorney General Eric Holder noting that it "is a matter of public record that Section 215, which is a public statute, has been the subject of secret legal interpretations . . . [contained in] opinions issued by the Foreign Intelligence Surveillance Court."[34] The letter noted that the American public has a "need and a right to know how [Section 215] is being interpreted, so that they can ratify or reject decisions made on their behalf."[35] The letter continued that "American laws . . . should not be made public only when government officials find it convenient. They should be public all the time, and every American should be able to find out

29. *See* 157 CONG. REC. S3,388–89 (daily ed. May 26, 2011) (statement of Sen. Udall).

30. *See* 157 CONG. REC. S3,360 (daily ed. May 25, 2011) (SA 384 to S. 1038, 112th Cong. § 3 (2011)).

31. Letter from Sen. Ron Wyden and Sen. Mark Udall, to Attorney General Eric Holder 1 (Sept. 21, 2011).

32. *Id.*

33. *Id.* at 1–2.

34. Letter from Sen. Ron Wyden and Sen. Mark Udall, to Attorney General Eric Holder 1 (Mar. 15, 2012).

35. *Id.* at 1–2.

what their government thinks those laws mean."[36]

In October 2011, on the tenth anniversary of the Patriot Act, the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) filed separate Freedom of Information Act (FOIA) lawsuits against the DOJ.[37] The lawsuits sought to uncover the "secret legal interpretation" of Section 215 about which elected officials had warned.[38] For nearly three years, the lawsuits yielded only limited information.

Early in the case, the ACLU sought partial summary judgment motion on the withholding of a single document.[39] The ACLU contended the document contained Section 215's secret legal interpretation; the government, for its part, claimed that the document only described classified surveillance techniques and did not, in fact, contain any legal interpretation.[40] After reviewing the document *in camera*, a judge in the Southern District of New York agreed, and granted partial summary judgment for the government.[41] While the case continued for the balance of the responsive documents, the suit largely languished.

EFF's suit fared little better. EFF identified a series of FISC opinions withheld by the government that, EFF argued, contained the secret interpretation of Section 215.[42] The government, for its part, claimed *everything* within the opinions was classified: the dates the opinions were issued, the topics of the opinions, even the number of pages that were

---

36. *Id.* at 2.

37. *EFF Sues for Answers About Patriot Act on Law's 10th Anniversary*, ELECTRONIC FRONTIER FOUNDATION (Oct. 26, 2011), https://www.eff.org/press/releases/eff-sues-answers-about-patriot-act-laws-10th-anniversary; Anna Estevao, *ACLU Sues Government to Find Out Secret Interpretation of Patriot Act*, ACLU (Oct. 26, 2011), https://www.aclu.org/blog/national-security/aclu-sues-government-find-out-secret-interpretation-patriot-act.

38. *Id.*

39. Mem. & Order, ACLU v. FBI, No. 11-cv-7562-WHP (S.D.N.Y. 2012), *available at* https://www.aclu.org/files/section215/DistrictCourtProceedings/sec215_order_granting_goverment_motion_for_summary_judgment_may_17_2012.pdf.

40. *Id.*

41. *Id.*

42. Notice of Mot. for Pl., Electronic Frontier Foundation v. United States Dep't of Justice, No. 4:11-cv-05221-YGR (N.D. Cal. 2013), *available at* https://www.eff.org/document/effs-opposition-and-cross-motion-summary-judgment.

in the opinions.[43] Although a court in the Northern District of California ordered the government to disclose *some* information about the opinions, three years after filing suit, the government's secret interpretation remained safely under wraps.[44]

The *Guardian*'s June 2013 article disclosed what the courts had refused to do—the program and its legal underpinnings. As a result of the disclosure of the call records program in the *Guardian*, and the government's confirmation of the program, there was no longer a sound basis for refusing to disclose the secret legal interpretations that the government relied on to support those programs. Consequently, EFF and ACLU's lawsuits resulted in the release of hundreds of pages of previously secret FISC opinions on Section 215.[45]

The proposals in this article, if implemented, can help prevent a similar scenario from occurring in the future.

II. THE PROBLEM OF SECRET (SURVEILLANCE) LAW AND THE TRADITIONAL WAYS TO AVOID IT

A. The Problem of Secret (Surveillance) Law

Broadly speaking, secret law obstructs democratic accountability and legitimacy.[46] By obstructing citizen oversight of the manner in which government officials interpret and implement the law, it is impossible to knowledgeably (1) reform the laws; (2) ratify interpretations

43. Mem. of P. & A. for Def., Electronic Frontier Foundation v. United States Dep't of Justice, No. 4:11-cv-05221-YGR (N.D. Cal. 2013), *available at* https://www.eff.org/document/department-justices-opposition-and-reply.

44. Order Re: Further Submission on Cross-Motion for Summary Judgment, Electronic Frontier Foundation v. Department of Justice, No. 4:11-cv-05221-YGR, (N.D. Cal. 2013), *available at* https://www.eff.org/document/courts-order-requiring-further-submissions-defendants.

45. *See, e.g.*, Trevor Timm, *Hundreds of Pages of NSA Spying Documents to be Released as Result of EFF Lawsuit*, ELECTRONIC FRONTIER FOUNDATION (Sept. 5, 2013), https://www.eff.org/deeplinks/2013/09/hundreds-pages-nsa-spying-documents-be-released-result-eff-lawsuit.

46. There is little need to dwell on the problems presented by secret law. As one commentator has noted, "condemnation of secret law seems too easy, because it is morally and politically over determined, after two centuries worth of the rhetoric and developing practice of liberalism and democratic self-government." Christopher Kutz, *The Repugnance of Secret Law*, UC BERKELEY SCHOOL OF LAW, http://law.usc.edu/centers/clp/papers/documents/Kutz.pdf.

of current law; or (3) hold political officials to account (whether through support or condemnation)[47] Without the pressure of accountability, democratic legitimacy, in turn, falls away.

The problem of secret law in the surveillance context deserves additional attention because the problems posed by secret law are exaggerated in the surveillance context. In general, the interpretation of laws by government officials cause government action that, in turn, has recognizable physical effects—interpretation of tax laws results in tax liens; traffic laws, traffic tickets; and so on. Indeed, even otherwise "secret" government action typically produces some physical manifestation of that action: for example, try as the government might to keep its drone strikes in the Middle East a secret, as public evidence and real world effects accumulated, government secrecy concerning those operations (and, relatedly, their legal justification) became increasingly difficult to shield from public scrutiny.[48]

Surveillance is different. As the Supreme Court recognized in *United States v. U.S. District Court* (*Keith* case), electronic surveillance—with its "broad and unsuspected governmental incursions into conversational privacy"—requires heightened attention.[49] Surveillance, unlike most forms of government action, is by its very nature clandestine. It can be difficult, if not impossible, to detect, and thus its public disclosure through observation is less likely.[50]

---

47. *Id.*

48. Cora Courrier, *How the Gov't Talks About A Drone Program It Won't Acknowledge Exists*, PROPUBLICA (Sept. 13, 2012), http://www.propublica.org/article/how-the-govt-talks-about-a-drone-program-it-wont-acknowledge. The CIA's drone program exemplifies the absurdity of the government's continued insistence on secrecy: secrecy is difficult when, for example, a Twitter feed (https://twitter.com/dronestream) publicly catalogues each reported government strike.

49. United States v. United States District Court, 407 U.S. 297, 313 (1972).

50. This is not to say that surveillance has no effect, particularly on those being surveilled. *See generally* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013). Obviously, and as the Supreme Court recognized in *Keith*, government incursions into conversational privacy are, themselves, one effect which must be guarded against. It is also not to say that it is impossible to detect electronic surveillance, depending on the method of surveillance employed. Finally, this is not to say surveillance is the only type of covert government action. Obviously, a great deal of government activity, particularly in the national security context, occurs covertly. However, I see no reason that the principles which this article advances—access to the legal

As new surveillance techniques or activities come to fruition, law enforcement officials are quick to fit them within existing legal authorities and frameworks with varying degrees of credibility. In the "competitive enterprise of ferreting out crime," [51] secrecy—both for surveillance techniques and their legal bases—is suggested to be a necessary evil: secrecy is necessary, it is argued, so that criminals cannot thwart legitimate government surveillance. As a corollary, secrecy for the technique is used to justify secrecy for the legal analysis. If the legal basis for an otherwise secret surveillance technique is disclosed, government officials argue, that would inevitably result in disclosure of the technique itself.[52]

This theory has justified the concealment of a great number of surveillance activities and a great many legal interpretations. Recent examples include: the suppression of information concerning law enforcement's use of Stingray devices;[53] secrecy in Office of Legal Counsel's memoranda concerning authoritative interpretations of federal surveillance law;[54] and, perhaps most saliently, the legal opinions of the FISC.[55] Each of these varieties of secret surveillance law has been perpetuated on the basis that disclosure of the legal rationale would, itself, reveal the technique.

---

principles animating surveillance—could not apply to other covert activities.

51. *Johnson v. United States*, 333 U.S. 10, 14 (1948).

52. *See e.g.*, Final Brief for Appellee at 42–47, Electronic Frontier Foundation v. U.S. Dep't of Justice, No. 12-5363 (11th Cir. June 7, 2013), *available at* https://www.eff.org/document/dojs-appellate-brief; Motion at 14, Electronic Frontier Foundation v. U.S. Dep't of Justice, No. 05221 (N.D. Cal. 2014), *available at* https://www.eff.org/document/doj-motion-summary-judgment-1.

53. Feds intervening to suppress disclosure of stingray records in FL; or recent muckrock article re: FBI rider in all stingray contracts that info must remain secret; Shawn Musgrave, *Before They Could Track Cell Phone Data, Police Had to Sign a NDA with the FBI*, MUCKROCK (Sept. 22, 2014), https://www.muckrock.com/news/archives/2014/sep/22/they-could-track-cell-phone-data-police-had-sign-n/.

54. The Editorial Board, *What Happened to Transparency?*, NEW YORK TIMES (Jan. 7, 2014), http://www.nytimes.com/2014/01/08/opinion/what-happened-to-transparency.html.

55. Charlie Savage & Laura Poitras, *How a Court Secretly Evolved, Extending U.S. Spies' Reach*, N.Y. TIMES (Mar. 11, 2014), *available at* http://www.nytimes.com/2014/03/12/us/how-a-courts-secret-evolution-extended-spies-reach.html.

A. Traditional Ways of Avoiding Secret Law and Their Shortcomings: Congressional Investigation, Discovery, Leaks, and FOIA

The government does not always rely upon secret legal interpretations of federal law and the Constitution. At least three mechanisms currently exist to counteract secret interpretations of federal law: Congressional investigation, discovery, leaks, and the Freedom of Information Act (FOIA). Through disclosures based on these three mechanisms, legal interpretations can then be tested in adversarial proceedings or reviewed and scrutinized in the court of public opinion. Either of these types of disclosure, in court or to the public, serves the ultimate goal of ensuring public ratification and legitimizing interpretations of law on which the government operates. But, as will be discussed, each of these mechanisms has its own disadvantages as well.

1. *Congressional Investigation*

Of all the methods of disclosing secret interpretations of law, Congressional investigation may be the most potent. Congress, obviously, is a coequal branch of government, empowered to investigate the actions of the executive branch.[56] This authority, in the past, has been powerfully exercised to uncover intelligence agency actions and their purported legal bases.

The Church and Pike Committees are the highest examples of the robust power of Congressional investigation to provide the public with information about the actions of intelligence agencies. Following a series of reports concerning illegal actions by intelligence agencies,[57] Congress convened the two committees to investigate the actions of the CIA, NSA, and FBI.[58] The hearings and reports of the committees resulted in the most expansive, and public, look at the actions

56. McGrain v. Daugherty, 273 U.S. 135, 174–175 (1927)

57. *See, e.g*., Seymour Hersh, *Huge C.I.A. operation reported in U.S. against antiwar forces, other dissidents in Nixon years*, NEW YORK TIMES (Dec. 22, 1974).

58. Gerald K. Haines, *The Pike Committee Investigations and the CIA, Studies in Intelligence (Winter 1998-99), available at* https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/winter98_99.

of American intelligence agencies in our nation's history.[59] The recommendations of the committees led to numerous reforms, including the creation of standing Congressional committees overseeing intelligence agency conduct and the passage of new laws, like the Foreign Intelligence Surveillance Act, to rein in intelligence agency conduct.[60]

The standing committees, in turn, have continued their oversight of intelligence agency conduct. At times, this oversight has lead to thorough and public reviews of intelligence agency conduct.[61] More often, however, committee oversight has meant closed door briefings and, at best, public hints at the edges[62] But, even with continued oversight of intelligence committees, it is clear that the mechanisms for preventing the development of secret law have failed. Section 215, a perfect example of secret agency reinterpretation, occurred under the careful watch of both Congressional intelligence committees.[63] The probable reasons for this breakdown—distorted classification policy, committee capture, institutional deficiencies, or other reasons[64]—are beyond the scope of this Article. But, suffice it to say, Congressional oversight, although a potentially potent tool, failed spectacularly and publicly in preventing the development of secret surveillance law.

2. Discovery

The first, and perhaps most common, method for compelled disclosure of the government's legal interpretations supporting law enforcement techniques is through disclosure

---

59. *See* Select Committee to Study Governmental Operations with Respect to Intelligence Agencies, S. Rep. No. 94-755 (1976) (7 volume report on actions of intelligence agencies).

60. *See* https://www.senate.gov/artandhistory/history/common/investigations/ChurchCommittee.htm.

61. *See, e.g.*, Senate Select Committee on Intelligence, Committee Study of the Central Intelligence Agency's Detention and Interrogation Program (Dec. 13, 2014)

62. *See supra* at 105–06.

63. *Id*.

64. Amy P. Zegart, The Roots of Weak Congressional Intelligence Oversight, TASK FORCE ON NATIONAL SECURITY AND LAW, *available at* http://media.hoover.org/sites/default/files/documents/FutureChallenges_Zegart.pdf; DENNIS MCDONOUGH ET AL., NO MERE OVERSIGHT, CONGRESSIONAL OVERSIGHT OF INTELLIGENCE IS BROKEN (2006).

during discovery in criminal and, to a lesser extent, civil cases. In the criminal context, the government is required to disclose the methods employed to obtain the evidence it will rely on at trial.[65] If the government relied on a novel surveillance technique or novel legal authority, a criminal defendant (with competent counsel) will challenge the legality of that technique in an attempt to suppress the evidence. And, in the course of briefing the suppression issue, the government's legal theories will necessarily be disclosed—and tested—in adversarial proceedings.[66] Civil cases, too, can allow for public disclosure of the government's legal interpretation supporting a particular technique.[67]

Examples are plentiful: in *United States v. Ringmaiden*, a criminal defendant challenged the government's use of a "Stingray"—a device that "catches" the International Mobile Subscriber Identity (IMSI) of cell phones in an area for the purpose of tracking an individual's movements.[68] In *United States v. Forrester*, a defendant challenged the use of an internet pen-register device.[69] Perhaps more prominently, in *Kyllo v. United States*, a criminal defendant challenged the warrantless use of thermal imaging technology that led to a conviction for marijuana cultivation.[70] And in *United States v. Jones*, the defendant challenged the government's use of GPS tracking to secure a conviction for drug conspiracy and distribution.[71]

But limiting disclosure of legal theories to those occurring in criminal cases leaves gaps in public understanding. This is so because prosecutors only disclose that a new technique has been used when the government

---

65. *See, e.g.*, Brady v. State of Maryland, 273 U.S. 83 (1963); Giglio v. United States, 405 U.S. 31 (1972).

66. Kevin Poulsen, *Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years*, WIRED (Apr. 16, 2009), http://www.wired.com/2009/04/fbi-spyware-pro/.

67. Although absent indisputable proof the surveillance has occurred—the government has used questions of standing to avoid addressing the substantive legality of surveillance. *See* Amnesty v. Clapper, 133 S. Ct. 1138 (2013).

68. Hanni Fakhoury, *Stingrays: The Biggest Technological Threat to Cell Phone Privacy You Don't Know About*, ELECTRONIC FRONTIER FOUNDATION (Oct. 22, 2012), https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy.

69. United States v. Forrester, 512 F.3d 500 (9th Cir. 2007).

70. Kyllo v. United States, 533 U.S. 27 (2001).

71. United States v. Jones, 132 S. Ct. 945 (2012).

intends to introduce that evidence or rely on evidence derived from the technique. And, as recent disclosures confirm, law enforcement often takes great pains to avoid disclosing that a particular technique has been used or has generated evidence derived from the technique.[72] This type of investigatory "laundering," in turn, precludes a public understanding, and adversarial testing, of the legal basis for the technique (even if the technique's legality has been reviewed internally within the executive branch).

Recent disclosures concerning the Drug Enforcement Agency's (DEA) use of NSA-derived information illustrates the problem. To avoid informing criminal defendants that information used in their arrest had been derived from NSA surveillance, DEA engaged in "parallel construction": that is, the collection of evidence, through independent and alternative means of investigation, originally obtained through NSA's surveillance programs.[73] The government has taken a similarly recalcitrant approach to its disclosure obligations under the FISA Amendments Act (FAA), a 2008 law that authorized broad, warrantless surveillance of international communications.[74] Not a single criminal defendant was notified that FAA surveillance had been used from the laws passage, in 2008, until September 2013.[75] Consequently, the government effectively obstructed review of the constitutionality of the law and the surveillance conducted under its authority. Aside from the Fifth and Sixth Amendment problems stemming from the government's secretive approach, the public suffers—it is blocked from understanding the legal authorities that animate government conduct.

A similar problem arises in the conduct of intelligence programs or techniques, especially those occurring abroad, that never give rise to criminal prosecution. Although not

---

72. *See, e.g.*, John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013), http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

73. *Id.*

74. 50 U.S.C § 1881(a).

75. Charlie Savage, *Federal Prosecutors, In A Policy Shift, Cite Warrantless Wiretapes As Evidence*, NEW YORK TIMES (Oct. 26, 2013), http://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html.

involving surveillance law, the government's legal rationale for the targeted killing of Americans' abroad amply demonstrates the dilemma. Given that the government was contemplating an extrajudicial killing of an American citizen, the chance that the legal justification for conducting that killing would arise in a criminal trial was, obviously, minimal. In the surveillance context, the government undertakes a great many surveillance techniques and procedures abroad, the vast majority of which will never lead to a criminal prosecution. Consequently, under current practices, the accompanying legal analysis may never see public disclosure.

3. Leaks

In general, there are two kinds of leaks[76]—authorized leaks and unauthorized leaks. For different reasons, neither is an ideal vehicle for eliminating secret law.

First, authorized leaks, done by government officials with the approval of the relevant policymakers, have a variety of purposes, from floating a proposed policy[77] to disclosing otherwise sensitive information that aids a particular policy or initiative.[78] The difficulty with relying on the authorized leak is that it depends wholly on the decision-making of policymakers. It thus entrusts the disclosure of the law to the same policymakers that chose to develop it in secret in the first instance. Therefore, the authorized leak is not a promising solution to combating secret law.

The unauthorized leak also does not offer a complete solution, but for different reasons. At the outset, there are

---

76. For a far more comprehensive treatment on the subject of leaks and their various types, see David Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512 (2013). Pozen describes and catalogues a far greater number of types of leaks than "authorized" and "unauthorized," however all identified types still seem to fall within one category or the other. *See id.* at 532.

77. This type of leak is often known as a trial-balloon leak. *See id.* at 532.

78. One example of this type of leak is the thwarting of a terrorist attack or the killing of a high-ranking terrorist leader. Often the operations, and the facts themselves, are classified, yet the success of these missions is often intentionally revealed to the press. *See, e.g.*, Greg Young & Karen DeYoung, *Al Queda airline bomb plot disrupted, U.S. says*, THE WASHINGTON POST (May 7, 2012), *available at* http://www.washingtonpost.com/world/national-security/cia-disrupts-airline-bomb-plot/2012/05/07/gIQA9qE08T_story.html.

obviously problems with depending on unauthorized leaks for the disclosure of secret law. Most obviously, it requires a person with knowledge or access to the law to leak documents; in the absence of a leaker, the public is beholden to the government's disclosure decisions. But, even when a leaker exists, unauthorized leaks carry risk. Although the unauthorized leak has the capacity to disclose secret law, an authorized leak's various permutations—from document dumps to leaks of single documents—often removes knowledgeable policymakers from the process of determining what will, and what will not, cause harm through disclosure. Consequently, the unauthorized leak risks overdisclosure of sensitive information. This is not to say that government officials do not, with regularity, speak in greatly hyperbolic terms about the damage that unauthorized leaks do to national security.[79] They do. But, even if regularly overstated, the concern is a legitimate one. It is quite easy to envision circumstances in which disclosure of government secrets could cause irreparable harm. This is so, even when the document disclosed consists solely of legal analysis. Invariably, that legal analysis would include discussion of specific facts or information that could reveal legitimately classified or sensitive information. Removing the government and relevant policymakers from the disclosure process entirely would thus threaten disclosure of sensitive information.

Of course, as a practical matter, established media outlets often work with the government before publishing leaked documents in order to withhold information the government claims cannot be disclosed.[80] In this respect, unauthorized leaks are an improvement over authorized leaks, in that a third-party (the media) examines the government's claims of harm to national security and makes decisions based on its own judgment. Nevertheless, that

79. *See, e.g.*, Jack Shafer, *Live and Let Leak*, FOREIGN AFFAIRS (2014), *available at* http://www.foreignaffairs.com/articles/140754/jack-shafer/live-and-let-leak (describing "irreparable harm" that would flow from the publication of plans for a hydrogen bomb and the Pentagon Papers, neither of which came to fruition).

80. *See, e.g.*, *A Note to Readers: The Decision to Publish Diplomatic Documents*, NEW YORK TIMES (Nov. 28, 2010), http://www.nytimes.com/2010/11/29/world/29editornote.html.

process is an imperfect one, too. First, media outlets can be swayed by hyperbolic government claims. For example, the *New York Times* delayed its publication of a story on warrantless wiretapping for nearly two years, apparently in response to government claims of harm to national security.[81] Second, although the judgment of publishers is interposed between the government and disclosure, it is not clear that publisher's judgment is the ideal one. Aside from possible subject-matter knowledge and (purported) journalistic neutrality, on its face, there is little more that redeems the judgment of a newspaper publisher over that of democratically accountable policymaker. Again, this is not to impugn journalists and the media. Professional journalists often exercise remarkable judgment about what should and should not be disclosed—often achieving a far more meaningful balance than government officials. But not all leaks are created equal; nor are all publishers of leaks. In the hands of less careful, or less interested, publishers, unauthorized disclosures serve as an imperfect vehicle for disclosure of secret law.

4. FOIA

An established but oft-maligned tool of public accountability is the FOIA. FOIA's "basic purpose," according to the Supreme Court, is no less than to "ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed."[82] The Act's primary purpose is disclosure not secrecy, and the law requires federal agencies to disclose records requested by any individual.[83] While exemptions from the Act's disclosure requirements exist—for example, for protecting law enforcement techniques,[84] and protecting "intelligence sources and methods"[85]—those

81. Margaret Sullivan, *Lessons in Surveillance Drama Redux*, THE NEW YORK TIMES (Nov. 9, 2013), *available at* http://www.nytimes.com/2013/11/10/public-editor/sullivan-lessons-in-a-surveillance-drama-redux.html.

82. NLRB v. Robbins Tire, 437 U.S. 214 (1978).

83. Dep't of Interior v. Klamath Water Users Protective Ass'n, 532 U.S. 1, 8 (2001).

84. 5 U.S.C. § 552(b)(7).

85. 5 U.S.C. § 552(b)(1).

exemptions are supposed to have a "narrow compass."[86]

In passing FOIA, Congress intended to open agency action to the scrutiny of the public.[87] To this end, both the provisions of FOIA and cases interpreting the law have evinced a powerful aversion to agency attempts to hide agency "law" from public disclosure. Indeed, "[o]ne of the principal purposes of the Freedom of Information Act is to eliminate secret law."[88] The affirmative portions of FOIA underscore the statute's aversion to secret law: agency's are affirmatively required to disclose "final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases;"[89] and "those statements of policy and interpretations" that have been adopted by the agency.[90]

For all the high-minded talk of exposing agency action to the light of day, FOIA, in practice, is also not without its limitations. Although FOIA broadly mandates disclosure and affirmatively requires disclosure of interpretations relied upon by the agency—federal agencies are often reluctant to observe the full requirements of the law. Consequently, a FOIA request for information may languish for months or even years, and even the onset of litigation does not guarantee disclosure of records. Additionally, courts have afforded near-absolute deference to agencies when those agencies assert that disclosure of information—even with redactions to protect sources and methods—would cause harm to national security or law enforcement surveillance techniques.[91] As a result of this deference, courts routinely allow the government to withhold documents, in their entirety, simply because portions of the documents may contain sensitive material.

Indeed, the government was able to conceal its interpretation of Section 215 for two years, despite the

---

86. Dep't of Justice v. Tax Analysts, 492 U.S. 136, 151 (1989).

87. NARA v. Favish, 541 U.S. 157, 171 (2004).

88. Jordan v. Dep't of Justice, 591 F.2d 753, 781 (D.C. Cir. 1978) (Bazelon, J., concurring) (citation omitted).

89. 5 U.S.C. § 552(a)(2)(A).

90. 5 U.S.C. § 552(a)(2)(B).

91. *See e.g.*, Frugone v. CIA, 169 F.3d 772, 775 (D.C. Cir. 1999). Because "courts have little expertise in either international diplomacy or counterintelligence operations, [they] are in no position to dismiss the [agency's] facially reasonable concerns" about the harm that disclosure could cause to national security.

existence of at least two separate FOIA lawsuits filed specifically to compel disclosure of that interpretation.[92] Seen in this light, FOIA may seem like an ineffective tool; however, as will be shown, with only slight alteration to current FOIA litigation practices, the government's ability to shield secret legal interpretations of surveillance law can be greatly diminished, without compromising legitimately protectable "sources and methods."

I. THE SOLUTION: THE TEARLINE VAUGHN INDEX

Public debate on the government's use of Section 215 was unduly constrained. The public could have readily been informed of the salient characteristics of the government's interpretation of the law—that the term "relevant" had been interpreted to authorize the production of millions of "irrelevant" records;[93] that those irrelevant records included the records of millions of law abiding Americans;[94] and that the FBI could obtain the orders, not for itself, but for other intelligence agencies—without disclosing the specifics of the Section 215 program.[95] This problem could have been avoided through the compelled production of unclassified summaries of this legal interpretation—a tearline *Vaughn*.

The tearline *Vaughn* is the combination of two types of documents: the "tearline" and the *Vaughn* index. First, a "tearline" is a tool already in use within the intelligence community. Essentially, tearlines are a way to disseminate information without revealing the classified information on which it is based.[96] Tearlines are portions of a document "that provide the substance of a more highly classified or controlled report without identifying sensitive sources, methods, or other operational information."[97] As one advocate for their greater use, Steven Aftergood of the

92. *See supra* note 37. Despite the existence of these lawsuits, the NSA's bulk collection of call records under Section 215 remained secret until the *Guardian*'s story in 2013.

93. *See* 50 U.S.C. § 1861.

94. *Id.*

95. *Id.*

96. Intelligence Community Directive 209, *Tearline Production and Dissemination* (Sept. 6, 2012), OFFICE OF THE DIRECTOR OF NAT'L INTELLIGENCE, *available at* https://fas.org/irp/dni/icd/icd-209.pdf.

97. *Id.*

Federation of American Scientists, has described them, tearlines refer "to the practice of segregating and withholding the most sensitive portions of a document, allowing the remainder to be 'torn off,' literally or figuratively, and widely disseminated."[98]

As recent practice has shown, it is often possible for the executive branch to disclose, in general terms, legal analysis concerning intelligence or law enforcement sources and methods without revealing the sensitive particulars of those methods. For example, the DOJ has released unclassified "white papers" on its legal interpretation of Section 215 and on the executive branch's authority to conduct targeted killings of citizens overseas.[99] These white papers are similar to tearlines in many respects. They deal, in general terms, with the substance of the legal analysis supporting the methods, without revealing the particular sources and methods at issue. For example, the White Paper on Section 215 does not disclose the particular telecommunication companies involved in the program; and, indeed, one could envision an even more abstracted version that dealt only with "business records" generally, not the particular telephone records at issue in the NSA's program.[100] Although Congress has indicated that the executive branch should employ tearlines with more frequency, it has not mandated their use in any particular circumstance.[101] However, without government creation of an unclassified summary for its own use, these types of publicly producible documents may not otherwise exist.

The litigation procedures already in place in FOIA can help fill this gap. The compelled production of documents, however, runs contrary to basic FOIA tenets. As a general rule, agencies are not required to create documents in response to a FOIA request that do not otherwise exist—with

98. Steven Aftergood, *DNI Directive Promotes Use of "Tearline" Documents*, FEDERATION OF AMERICAN SCIENTISTS (Sept. 28, 2012), *available at* http://fas.org/blogs/secrecy/2012/09/tearlines/.

99. *Department of Justice White Paper*, NBC NEWS MEDIA, http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf; Administration White Paper, *Bulk Collection of Telephony* (Aug. 9, 2013), https://www.eff.org/files/filenode/section215.pdf.

100. *See generally id.*

101. *See* 6 U.S.C. § 485(d)(1).

one common exception: the *Vaughn* Index. Named for the seminal DC Circuit decision, *Vaughn v. Rosen*, the *Vaughn* index requires government agencies to create an index of withheld documents, "specifying in detail which portions of the document are disclosable and which are allegedly exempt."[102]

As the D.C. Circuit recognized in *Vaughn*, the "traditional adversary nature of our legal system's form of dispute resolution" is "seriously distort[ed]" in the typical FOIA case.[103] This is so because, in ordinary civil litigation, "the facts relevant to a dispute are more or less equally available to adverse parties."[104] But, in FOIA cases, it is anomalous, but obviously inevitable, that the party with the greatest interest in obtaining disclosure is at a loss to argue with desirable legal precision for the revelation of the concealed information. Obviously the party seeking disclosure cannot know the precise contents of the documents sought; secret information is, by definition, unknown to the party seeking disclosure. In many, if not most, disputes under the FOIA, resolution centers around the factual nature, the statutory category, of the information sought.[105]

The *Vaughn* index, then, is used to recalibrate that imbalance—however slightly. The *Vaughn* index "describe[s] the document withheld or any redacted portion thereof, disclosing as much information as possible without thwarting the exemption's purpose."[106] And the *Vaughn* index falls outside of FOIA's general prohibition against compelled creation of documents because the index is actually a procedural litigation tool—a product of the courts' inherent authority to regulate the parties before it. It is akin to a privilege log—a procedural tool common in typical civil discovery.

The tearline *Vaughn*, then, is a combination of the attributes of the tearline and the *Vaughn* index. First, agencies are able to produce unclassified "summaries," even of classified content and an already-established procedure

102. Vaughn v. Rosen, 484 F.2d 820, 827 (D.C. Cir. 1973).
103. *Id.* at 824.
104. *Id.*
105. *Id.*
106. King v. United States Dep't of Justice, 830 F.2d 210 (D.C. Cir. 1987).

exists for doing so—the tearline. Second, in spite of FOIA's general prohibition on the creation of documents, the federal courts are empowered to order the government to create documents in FOIA cases—and, indeed, often do—particularly where fairness requires it.

The tearline *Vaughn* can be implemented in those instances where a court is caught between accommodating the executive branch's need to protect sensitive intelligence "sources and methods" and honoring Congress' purpose, in passing FOIA, of eliminating agency "secret law." If we accept that FOIA's primary purpose is to root out secret law within government,[107] it follows that courts should not casually accept government attempts to shield entire documents containing controlling agency legal interpretations, even if those documents might contain *some* legitimately classifiable information. Courts should be willing to push the executive branch to be as forthcoming as possible when the documents are believed to contain agency law. A tearline *Vaughn* accomplishes precisely that.

Indeed, such a compelled tearline may be the only method to ensure government compliance with another requirement of FOIA—the obligation to segregate and release non-exempt information.[108] While the government often contends that redaction of sensitive information would yield only incomprehensible fragments, such claims are less credible where the document consists primarily of legal analysis. Cases, statutes, and legal principles—divorced from their specific factual bases—can be disclosed without compromising specific sources or methods. Indeed, the tearline *Vaughn* preempts this argument. Faced with choice of a purportedly incomplete redacted version, or a tearline *Vaughn*—the government should welcome the opportunity to provide a more fulsome explanation in tearline format.

The procedure for litigating the propriety and completeness of the tearline *Vaughn* would be similar to current FOIA litigation practices. In current FOIA litigation, a FOIA plaintiff is able to challenge the adequacy or

---

107. Public Citizen, Inc. v. OMB, 598 F.3d 865, 871 (D.C. Cir. 2010)("FOIA provides no protection for such 'secret law' developed and implemented by an agency.").

108. 5 U.S.C. § 552a(b).

sufficiency of the government's *Vaughn* index.[109] That is, the requester can contest that the government has not disclosed "as much information as possible" about the withheld documents.[110] The court then reviews the *Vaughn*, at times, the withheld documents and decides if the government has satisfied its obligation. An identical procedure could function with a tearline *Vaughn*. After submitting the tearline, the parties could dispute whether the government had disclosed "as much information as possible" about the withheld legal analysis.[111] A reviewing court (in accordance with FOIA's current procedures)[112] could examine the original, classified legal analysis *in camera*, comparing it to the tearline version submitted by the government, to settle whether its disclosure obligations had been satisfied. Such a procedure would ensure both that the public has the information it needs to critically assess the government's legal interpretation while at the same time maintaining the secrecy of any legitimately sensitive sources and methods.[113]

The tearline *Vaughn* is preferable to Congressional investigations, alone, because it marshals the authority of two branches of the federal government—Congress and the judiciary.[114] The tearline *Vaughn* avoids the problem of selective disclosure provided through discovery. A tearline *Vaughn* could be created about any surveillance technique the government is known to use or any provision of public law. This process also better addresses the problem posed by the case of unauthorized leaks—leaving to the judgment of

---

109. *See* Davin v. United States Dep't of Justice, 60 F.3d 1043, 1065 (3d Cir. 1995) (remanding case for further proceedings and suggesting that another, more detailed *Vaughn* Index be required); Church of Scientology Int'l v. United States Dep't of Justice, 30 F.3d 224, 239–40 (1st Cir. 1994); Wiener v. FBI, 943 F.2d 972, 979 (9th Cir. 1991) (remanding case for a more thorough *Vaughn* Index).

110. *King*, 830 F.2d at 224.

111. *Id.*

112. 5 U.S.C. § 552(a)(4)(B).

113. One shortcoming of the tearline Vaughn solution is its availability only through litigation. Thus, disclosure would be limited to those with the resources to compel it. However, the existence of some solution is preferable to the status quo and, eventually, similar types of disclosures could be incorporated into regular agency responses to FOIA requests—or mandated by Congress.

114. Congress, of course, passed FOIA and has encouraged the executive branch, by statute, to use tearlines.

media and publishers what information should be disclosed. While judges may lack the subject-matter knowledge of many journalists, federal judges rightly claim the same apparent neutrality. In addition, the federal judiciary is at least a formal part of our constitutional structure, lending its role as arbiter of disclosure an air of democratic legitimacy that newspaper publishers otherwise lack. Applying the tearline Vaughn to the case of Section 215 demonstrates its potential. As described above, in the context of Section 215, the normal channels of public access failed. The government was able to conceal from public disclosure for nearly eight years Section 215's unprecedentedly broad interpretation and implementation—in spite of Congressional oversight of its use, Section 215-derived evidence's use in a criminal prosecution, and in spite of two separate FOIA lawsuits directed at the interpretation. When the levee broke in June 2013, the government's most cherished secrets, including Verizon's participation in the program, came pouring out.

But the buildup in secrets behind the levee was unnecessary. The government could readily have provided more information about the government's interpretation without compromising the purported information it was trying to protect. For example, the government could readily have provided more detailed information about its definition of "relevance."[115] The only insight the government previously revealed concerning Section 215's interpretation was that it was "similar to a grand jury subpoena."[116] But, as the government well knew, no grand jury subpoena in the history of the Republic was as broad as even a single Section 215 order. Such understatement served only to deflect criticism and scrutiny, to conceal the government's interpretation, and to block the public from meaningfully debating the propriety of the statute.

All the government needed to disclose was the fact that,

115. This, of course, presumes that the government actually had conducted such an interpretation prior to the disclosures. Sadly, it is not always the case that a searching legal review of a particular technique is performed prior to its use.

116. Letter from Sen. Ron Wyden & Sen. Mark Udall, to Eric Holder, Attorney General of United States Department of Justice (Sept. 21, 2011), *available at* http://www.wyden.senate.gov/download/?id=a3670ed3-9f65-4740-b72e-061c7de83f75&download=1.

under the government's interpretation, a single Section 215 order could be used to obtain records concerning millions of Americans, almost all of whom would have no connection whatsoever to terrorism. They failed to, however, for pragmatic reasons: they likely knew that such a disclosure would lead to public outcry and the elimination of the program. And, such evasiveness speaks to the democratic legitimacy of such a law or interpretation.

That type of disclosure would have revealed very little operationally-sensitive information about the call records collection program: it would not have revealed that the government was collecting call records, let alone doing so in bulk; it would not have revealed the providers that were turning over call records; and it would not have revealed the targets of the investigation.[117] It would only have revealed that the government had interpreted its authority under Section 215 to allow it to obtain records on millions of Americans—the very aspect of the program that sparked such broad public outrage.

CONCLUSION

At least with respect to the Section 215 program, many of these "unauthorized" disclosures could have been avoided with more enlightened disclosure policies by Congress, the Executive branch, or the courts. A more tailored disclosure policy, such as that provided through a tearline *Vaughn*, would have protected the government's sources, methods, and targets of investigations while still allowing the public to engage in a meaningful debate about its use. Furthermore, the public could compel the government to disclose how it *interpreted* the law without disclosing how it *implemented* the law.

The tearline *Vaughn* system cannot claim to be a perfect system. But, while there may be some difficult cases around the edges, for the vast majority of techniques of intelligence programs, the legal principles animating the programs can be discussed at some level of abstraction without disclosing sources and methods. And that is precisely the role the tearline *Vaughn* can provide.

---

117. Indeed, the targets remain classified today.