NOTHING TO FEAR OR NOWHERE TO HIDE: COMPETING VISIONS OF THE NSA'S 215 PROGRAM

SUSAN FREIWALD*

INTRODUCTION 310
I. THE 215 PROGRAM 313
II. DIVERGENT ASSESSMENTS OF THE COSTS AND BENEFITS OF THE 215 PROGRAM 316
A. Bulk Surveillance Benefits 316
B. Bulk Surveillance Costs 318
C. Costs of Not Conducting Surveillance 319
III. DIVERGENT APPROACHES TO THE LEGALITY OF THE 215 PROGRAM 320
A. Legality of the 215 Program Under FISA 320
B. Legality of the 215 Program Under the Fourth Amendment 322
1. Is Bulk Collection a Fourth Amendment Search? 322
2. Fourth Amendment Reasonableness 324
C. Legality of the 215 Program Under the First Amendment . 326
IV. DIVERGENT APPROACHES TO WHAT CONSTITUTES ABUSE 328
A. Program Proponents Define Abuse Narrowly 328
B. Program Opponents Define Abuse Broadly 328
1. Not Following Procedures as an Abuse 328
2. Mission Creep as an Abuse 329
3. Does Government Possession of Data Constitute an Abuse? 330
4. What to Assume About Abuses in the Absence of Information About Them 330
CONCLUSION 331

* Susan Freiwald, Professor of Law, University of San Francisco School of Law. I thank research librarian John Shafer, my research assistants Caleb Braley and Everett Monroe and the editors at the Colorado Law Technology Journal. I also thank the following people for their helpful feedback: H. Bryan Cunningham, Lothar Determann, Peter Micek, Paul Ohm, Emily Poole, Erik Shallman, Elif Somnez, and Ben Wizner. Any errors are entirely my own.

INTRODUCTION

Two divergent visions of the harm from the National Security Agency's (NSA's) bulk data collection competed for the public's attention in the wake of the publication of Edward Snowden's leaked documents in June of 2013.[1] Proponents of the Section 215 metadata program[2]—executive branch representatives, intelligence agency leaders, members of the legislature and other supporters—largely encouraged us not to worry. They argued that the terrorist threat amply justifies bulk surveillance for national security purposes, which has been effective in keeping us safe from attack. In hearings, press interviews, and court submissions, they maintained that those concerned about the program do not understand how it works.[3] Importantly, program proponents explained that agents have acted within statutory and constitutional bounds, subject to meaningful oversight,[4] resulting in minimal abuses.[5] With full information, they claimed, people would recognize that any harm the program causes is justified by the program's benefits.[6] Those historically opposed to government surveillance—writers, technologists, lawyers, and advocacy groups—remained skeptical of such reassurances.

The newly released documents provided a rare opportunity to learn the details of NSA surveillance. Previous challenges[7] to NSA

1. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. The research for this essay is concentrated on the period preceding and just following the January 17, 2014 Symposium of the Silicon Flatirons Center for Law, Technology, and Entrepreneurship: New Frontiers of Privacy Harm, at which I was a panelist.

2. The program proceeds under Section 215 of the USA PATRIOT Act. *See infra* Part I. For information on the programmatic warrant program that involves the content of communications and largely overseas communications, see 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), *available at* http://www.fas.org/irp/offdocs/pclob-215.pdf.

3. *See, e.g.*, Eli Lake, *Spy Chief: We Should've Told You We Track Your Calls*, DAILY BEAST (Feb. 17, 2014), http://www.thedailybeast.com/articles/2014/02/17/spy-chief-we-should-ve-told-you-we-track-your-calls.html ("In the interview [Director of National Intelligence] Clapper said the 215 program was not a violation [of] the rights of Americans. 'For me it was not some massive assault on civil liberties and privacy because of what we actually do and the safeguards that are put on this,' he said.").

4. *See infra* Part III (describing the legal precedents and accompanying arguments).

5. *See infra* Part IV (discussing the various definitions of "abuses").

6. *See infra* Part II. *Cf.* Lake, *supra* note 3 (contending that the American people would surely have approved of the 215 program had they known more about it earlier).

7. *See, e.g.*, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (denying the government's motion to dismiss claims alleging that telecommunication provider violated class members' constitutional and statutory rights by sharing their phone calls and records with the NSA). I co-authored an amicus brief in support of the class members.

surveillance, reported in the press,[8] had failed to yield significant disclosures before being dismissed.[9] After the Snowden releases, by contrast, intelligence officials confirmed the content of several classified documents and also released a substantial amount of new information.[10] Two groups of experts—the Privacy and Civil Liberties Oversight Board (PCLOB) and the President's Review Group on Intelligence and Communications Technologies (President's Review Group)—engaged in extensive fact-gathering exercises[11] and then issued lengthy reports detailing the 215 program and its legal and policy justifications.

Detailed knowledge of the inner workings of the NSA programs did not assuage all concerns; intense opposition to the program—spearheaded by civil liberties advocacy groups—formed immediately. Three such groups, the American Civil Liberties Union, the Electronic Frontier Foundation, and the Electronic Privacy Information Center, brought legal challenges to the 215 program.[12] Though appeals are pending, one district court has found the 215 program to violate the Fourth Amendment and enjoined its operation.[13] Two others have upheld the 215 program's constitutionality.[14]

8. David S. Kris, *On the Bulk Collection of Tangible Things*, LAWFARE RES. PAPER SERIES Sept. 29, 2013, at 3–4 (listing newspaper articles); James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=1&.

9. *See* Hepting v. AT&T Corp., 539 F.3d 1139 (9th Cir. 2008) (remanding in light of the FISA Amendments Act of 2008, which granted immunity to providers alleged to have given communications information to the NSA illegally).

10. The government posted opinions of the FISC, statements of agency officials, memoranda of agency procedures, whitepapers of legal positions, transcripts of congressional hearings, and videos of speeches. *See* IC ON THE RECORD, http://icontherecord.tumblr.com/ (last visited Oct. 1, 2014). Former Assistant Attorney General for National Security David Kris thoroughly documented and analyzed the early government disclosures. *See* Kris, *supra* note 8, at 6 n.24; *see also* Marty Lederman, *The Kris Paper, and the Problematic FISC Opinion on the Section 215 "Metadata" Collection Program*, JUST SECURITY (Oct. 1, 2013, 5:25 PM), http://justsecurity.org/2013/10/01/kris-paper-legality-section-215-metadata-collection/ (discussing the tremendous value of Kris's article).

11. DAVID MEDINE ET AL., 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 4–5 (2014) [hereinafter PCLOB REPORT], *available at* http://www.fas.org/irp/offdocs/pclob-215.pdf; *see also* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 277–81 (2013) [hereinafter REVIEW GROUP REPORT], *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

12. Complaint, First Unitarian Church of L.A. v. NSA, No. 13-3287 (N.D. Cal. July 16, 2013); Complaint, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *appeal docketed*, No. 14-42 (2d Cir. Jan. 6, 2014); Petition for Writ of Mandamus and Prohibition, *In re* Elec. Privacy Info. Ctr., 134 S. Ct. 638 (2013) (No. 13-58); Klayman v. Obama, 957 F. Supp. 2d 1, 7 n.2 (D.D.C. 2013) (collecting cases).

13. *Klayman*, 957 F. Supp. 2d at 43.

14. ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (finding that, had the court

The recent conflict has revealed that the proponents and opponents of Section 215 view the program in diametrically opposed ways. Program proponents see a vital intelligence program operating within legal limits, which has suffered a few compliance issues that were remedied by a well-functioning oversight regime. Program opponents see the same program as unauthorized and unconstitutional, yielding minimal benefits, and subject to significant abuses and insufficient oversight. Part of the disjunction reflects differing interpretations of the law, but much of it stems from a deep-seated lack of trust. For example, surveillance proponents tend to view civil libertarian activists as motivated by ideology and not amenable to persuasion by facts or reason.[15] They find frustrating the lack of credit they get for their own efforts to protect civil liberties.[16] Civil libertarian activists regard secret surveillance as a request that they merely "trust the government." They cite current and historical abuses of the surveillance power in this country and elsewhere as reason to refuse to do so.[17] I argue that each side's lack of trust in the other leads to the use of the same words to mean entirely different things.

This essay proceeds in the following manner. Part I provides a brief overview of the 215 program. Part II compares the proponents' cost-versus-benefit calculations to opponents' calculations. Part III considers how differently each group assesses the legality of the 215 program, considering both statutory authorization and the relevant constitutional provisions. Part IV compares each side's understanding of what it means to abuse the surveillance power, which depends crucially on the issues raised in the prior Parts. Because program opponents view it as ineffective and illegal, its very operation abuses civil liberties. Program proponents perceive no abuses when agents engage in legally authorized and justified surveillance. This essay concludes that whatever happens to the 215 program will not likely resolve the manner in which the

reached those issues, the plaintiffs would have failed to allege statutory violations); Smith v. Obama, 2014 WL 2506421, at *4 (D. Idaho June 3, 2014) (dismissing challenges, but describing the *Klayman* decision as a good template for a Supreme Court decision that the 215 program is unconstitutional).

15. *See*, *e.g.*, *Oversight of the Administration's Use of FISA Authorities: Hearing Before the H. Comm. on the Judiciary*, 113th Cong. 75 (2013) [hereinafter *July 2013 Hearings*] (statement of Stewart A. Baker, former NSA General Counsel) ("The privacy advocates who tend to dominate the early debates about government and technology suffer from a sort of ideological technophobia, at least as far as the government is concerned.").

16. *See, e.g.*, *id.* at 83 (statement of Stewart A. Baker) (contending that the three branches of government have "bent over backwards to protect" Americans' privacy while "conducting intelligence on the frontier of technology," but "large parts of the body politic are reluctant to trust classified protections" and "irresponsible advocates" have "distort[ed] the debate over our intelligence programs").

17. *See infra* note 107.

program's proponents and opponents talk past each other. Yet use of a common language could increase understanding, and even trust, and it would surely enhance opportunities for constructive engagement among the parties themselves and the greater public.

I. THE 215 PROGRAM

Pursuant to the 215 Program, the NSA collects call detail records from the large telecom providers pertaining to calls into, out of, and within the United States. A Foreign Intelligence Surveillance Court (FISC) order served on Verizon, which surfaced in the first Snowden disclosure, details the following as information collected: "comprehensive routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile Station Equipment Identity (IMEI), etc.), trunk identifier, telephone calling card numbers, and time and duration of calls."[18] The orders refer to the data collected as "metadata," or information about the telephone calls apart from the content of the calls.[19] In litigation, lawyers for the NSA have argued that the program requires the disclosure of all or substantially all of the metadata available for calls made within the United States.[20] 215 orders do not authorize the acquisition of metadata associated with Internet communications; however, agents did collect such information under a similar program until 2011.[21] The NSA reportedly abandoned its Internet metadata

18. Secondary Order, *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. 13-80, slip. op. at 2 (FISA Ct. Apr. 25, 2013), *available at* http://www.theguardian.com/world/interactive/2013/jun/06/ verizon-telephone-data-court-order. It may be that metadata includes data relating to text messages as well as phone calls. *Klayman*, 957 F. Supp. 2d at 35 n.56 (raising that possibility).

19. Program opponents have argued that metadata can reveal as much as the content of communications. *See, e.g.*, Memorandum of Law in Support of Plaintiff's Motion for a Preliminary Injunction at 18–19, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *appeal docketed*, No. 14-42 (2d Cir. Jan. 6, 2014) [hereinafter Plaintiff Memorandum in *Clapper*]. Others have disputed that claim. *See, e.g.*, PCLOB REPORT, *supra* note 11, at 211 (separate statement of Board Member Rachel Brand).

20. *See* Defendant's Memorandum of Law in Opposition to Plaintiff's Motion for a Preliminary Injunction at 16–24, *Clapper*, 959 F. Supp. 2d 724 [hereinafter Government Memorandum in *Clapper*]. One media report suggested that the 215 program acquired information on only a fraction of calls because it targeted only some communications providers. Ellen Nakashima, *NSA Is Collecting Less than 30 Percent of U.S. Call Data, Officials Say*, WASH. POST (Feb. 7, 2014), http://www.washingtonpost.com/world/national-security/nsa-is-collecting-less-than-30-percent-of-us-call-data-officials-say/2014/02/07/234a0e9e-8fad-11e3-b46a-5a3d0d2130da_story.html. *But see Clapper*, 959 F. Supp. 2d at 735 ("[T]he Government has acknowledged that it has collected metadata for substantially every telephone call in the United States since May 2006.").

21. REVIEW GROUP REPORT, *supra* note 11, at 97, 97 n.91 (explaining that agents used

program because it was not cost-effective.[22] Recently published 215 orders specifically prohibit the collection of cell site location information.[23] Intelligence officials have confirmed, however, that a pilot program permitted the acquisition of some location information in the past.[24]

Under the 215 program, a judge on the FISC issues or renews a primary order every 90 days,[25] which authorizes the NSA to issue secondary orders to telecommunication providers compelling them to disclose the requested metadata to the NSA.[26] The primary orders, which are significantly longer than secondary orders, spell out minimization requirements that limit agents' access to and dissemination of the metadata. They also specify oversight mechanisms and other protections.[27]

After telecommunications providers deliver information to the NSA—which they do on an ongoing, daily basis—NSA agents turn the data into readable form.[28] Then, twenty-two trained and approved agents have authorization to query the data, using selected "seeds"—usually telephone numbers—of those people for whom there is reasonable and articulable suspicion ("RAS") of an association with an identified terrorist group.[29] NSA agents may then engage in "contact-chaining," which means they may query the numbers (or other identifiers) called by

the pen register and trap-and-trace authority to obtain internet metadata until 2009 but then suspended the program in 2009 before restarting it in 2010).

22. *Id.* at 97 n.91 ("NSA Director General Keith Alexander decided to let the program expire at the end of 2011 because, for operational and technical reasons, the program was insufficiently productive to justify its cost.").

23. *See, e.g.*, Primary Order at 3 n.1, *In re* Application of the Fed. Bureau of Investigation Requiring the Production of Tangible Things From [Redacted], No. BR 13-109 (FISA Ct. Oct. 11, 2013) [hereinafter *FISC Primary Order*] (Eagan, J.) ("Furthermore, this Order does not authorize the production of cell site location information (CSLI).").

24. *See* Charlie Savage, *In Test Project, N.S.A. Tracked Cellphone Locations*, N.Y. TIMES (Oct. 2, 2013), http://www.nytimes.com/2013/10/03/us/nsa-experiment-traced-us-cellphone-locations.html?_r=0; PCLOB REPORT, *supra* note 11, at 156 n.558 (confirming collection of cell site information in 2010 and 2011).

25. The first FISC opinion approving of the 215 bulk metadata collection dates from 2006. PCLOB REPORT, *supra* note 11, at 9.

26. *FISC Primary Order*, *supra* note 23, at 5.

27. *Id.* Amended Memorandum Opinion at 11, *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109 (FISA Ct. Aug. 29, 2013) [hereinafter *FISC 2013 Opinion*] (Eagan, J.) (explaining that the Court would not have approved the bulk production order without the Primary Order's "detailed restrictions on the government through minimization procedures").

28. *FISC Primary Order*, *supra* note 23, at 5–6.

29. ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 5 (2013) [hereinafter ADMIN. WHITE PAPER], *available at* http:// apps.washingtonpost.com/g/page/politics/obama-administration-white-paper-on-nsa-surveillance-oversight/388/. The seeds can be other identifiers besides telephone numbers. *Id.*

and that called the seed number.[30] Prior to February of 2014, the NSA engaged in three-hop analysis; afterwards, it reportedly is limited to two-hop analysis.[31] Numbers directly in contact with the seed identifier are in the first "hop." The second hop includes the set of numbers in direct contact with first hop contacts, and the third hop refers to the set of numbers found to be in direct contact with the second hop contacts.[32] NSA officials reported using fewer than 300 seed identifiers in 2012,[33] but the number of query results would be substantially larger and depend on the number of contacts of the seed and its contacts. For example, if the seed number had 75 contacts, and each contact had 75 new contacts, three-hop analysis of the seed would yield 420,000 records of telephone numbers and associated calling information.[34]

Much of the discussion after the disclosures focused on the bulk collection of metadata and the subsequent focused querying subject to the RAS limitation. But it is important to understand that the results of the queries, including all of the information generated by pursuing contacts, are deposited for analysis into a different database, called the "corporate store."[35] Information in the corporate store is open to querying based on non-RAS terms, integration with data from other programs, and "other analytic methods and techniques."[36] FISC primary orders, however, require that such analysis be for valid foreign intelligence purposes.[37] In its January 2014 report, PCLOB estimated that the corporate store had records involving over 120 million telephone numbers.[38] Although NSA analysts may conduct relatively unfettered analyses of corporate store data,[39] they may share the results of their analyses with the FBI and other intelligence agencies only when they

30. Klayman v. Obama, 957 F. Supp. 2d 1, 18 (D.D.C. 2013); *see also* Kris, *supra* note 8, at 13 n.54 (describing contact-chaining).

31. *Joint Statement by Attorney General Eric Holder & Director of National Intelligence James Clapper on the Declassification of Renewal of Collection Under Section 215 of the USA PATRIOT Act (50 U.S.C. Sec. 1861)*, IC ON THE RECORD (Mar. 28, 2014), http://icontherecord.tumblr.com/post/81013190566/joint-statement-by-attorney-general-eric-holder.

32. *Admin. White Paper*, *supra* note 29, at 3–4.

33. *Id.* at 4.

34. PCLOB REPORT, *supra* note 11, at 29; *see also Klayman*, 957 F. Supp. 2d at 16 (calculating that a query with 100 contacts at each hop will generate 1,000,000 records).

35. PCLOB REPORT, *supra* note 11, at 29–31; ADMIN. WHITE PAPER, *supra* note 29, at 13 ("NSA employs a multi-tiered process of analyzing the data . . . ."). Metadata that has been collected but not yet subjected to querying is stored in the "collection store." *FISC Primary Order*, *supra* note 23, at 11.

36. PCLOB REPORT, *supra* note 11, at 30–31.

37. *FISC Primary Order*, *supra* note 23, at 11.

38. PCLOB REPORT, *supra* note 11, at 30–31.

39. For example, searches of the corporate store are not subject to audit. *FISC Primary Order*, *supra* note 23, at 7 n.6.

meet certain dissemination standards.[40]

II. DIVERGENT ASSESSMENTS OF THE COSTS AND BENEFITS OF THE 215 PROGRAM

Proponents of the 215 program do not entirely resist application of a cost/benefit rubric to assess the program's worth. At the same time, program opponents do not deny the dangers that terrorist attacks pose or the value of surveillance, per se, in protecting our nation. Yet the two groups make widely divergent calculations when they weigh the benefits against the costs of the 215 program.

A. Bulk Surveillance Benefits

Program opponents would count as a benefit the value surveillance provides in yielding actionable intelligence about terrorist threats and information about foreign spies. But they would argue that the benefits from national security surveillance are significantly more attenuated when the surveillance yields information about foreign intelligence[41] that is more broadly defined to include information pertaining to foreign affairs.[42]

Relatedly, program opponents have argued that the 215 program has been ineffective because it has yielded no information critical to preempting a terrorist attack on our nation.[43] They count surveillance as beneficial, moreover, only when it provides information not otherwise available from traditional investigative sources.[44] Opponents thus

40. *Admin. White Paper*, *supra* note 29, at 4 ("Analysts must apply the minimization and dissemination requirements and procedures specifically set out in the [FISC's] orders before query results, in any form, are disseminated outside the NSA."); s*ee also infra* note 129.

41. Obama Administration Presidential Policy Directive 28 (PPD-28): Signals Intelligence Activities n.2 (Jan. 17, 2014) [hereinafter *Policy Directive 28*] (noting that foreign intelligence includes information broadly pertaining to the activities of foreign countries and organizations).

42. *See, e.g.*, Harley Geiger, *Four Key Reforms for NSA Surveillance*, CTR. FOR DEMOCRACY & TECH. BLOG (Mar. 14, 2014), https://cdt.org/four-key-reforms-for-nsa-surveillance/ (complaining about NSA surveillance, under a different program, that relates to "foreign intelligence," broadly defined).

43. *See, e.g.*, Peter Bergen et al., *Do NSA's Bulk Surveillance Programs Stop Terrorists?*, NEW AM. FOUND. (Jan. 13, 2014), http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0_0.pdf ("Surveillance of American phone metadata has had no discernable impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity.").

44. *See, e.g.*, Plaintiff Memorandum in *Clapper*, *supra* note 19, at 35 (quoting Sens. Wyden and Udall) (calling the need for the "mass call-tracking program" into question because it does not provide "'any uniquely valuable intelligence'"); PCLOB REPORT, *supra* note 11, at 168–70. *Cf.* 18 U.S.C. § 2518(1)(c) (2012) (prohibiting wiretapping unless less intrusive investigative methods are ineffective).

accorded considerable skepticism to proponents' initial claim that the 215 program (along with another program) had been valuable in 54 counterterrorism cases.[45] The PCLOB report eventually concluded that the 215 program had yielded information unavailable from other investigative methods in only one case.[46] Because that case involved the contribution of $8,500 to a terrorist network rather than a plan threatening imminent violence, it did not establish the program's efficacy for the majority of PCLOB members and other program opponents.[47]

Those who have spoken in support of the program have taken a much broader view of its benefits. To them, the program yields benefits even if it confirms information available from other sources, because by doing so it buttresses those sources' credibility.[48] In addition, they argue that information that clears particular suspects of terrorist activity permits agents to shift resources towards investigating more valuable targets and cease the investigation of innocent people.[49] Rather than viewing them as wasted or ineffective, program proponents view database queries that reveal no threats to the United States as providing the benefit of peace of mind that the agents have not missed something.[50]

The two groups have fundamentally different views of the time horizon over which one should tally the benefits of the 215 program. Program opponents view the fact that the program has apparently yielded so little independent evidence of actual intelligence in its seven years of operation as evidence of insufficient benefits—the program should have much more to show for itself by now.[51] Program supporters argue that the program's performance to date does not indicate what it will do in the future—under this view, the prospect for future usefulness is a significant present value.[52]

45. *See* PCLOB REPORT, *supra* note 11, at 145; Klayman v. Obama, 957 F. Supp. 2d 1, 41 n.65 (D.D.C. 2013).

46. PCLOB REPORT, *supra* note 11, at 152; Bergen et al., *supra* note 43, at 2.

47. *See* PCLOB REPORT, *supra* note 11, at 152–53; *id.* at 168 (concluding that the 215 program had not demonstrated enough efficacy to justify its costs to privacy and civil liberties); Bergen et al., *supra* note 43, at 2.

48. *See generally* PCLOB REPORT, *supra* note 11, at 147–48 (listing seven possible ways to measure the efficacy of the 215 program).

49. *See, e.g.*, *July 2013 Hearings*, *supra* note 15, at 10 (testimony of John C. Inglis, NSA Deputy Director) (describing how useful intelligence focuses and sharpens the collection of additional data).

50. *See, e.g.*, PCLOB REPORT, *supra* note 11, at 212 (separate statement of Board Member Elizabeth Collins Cook).

51. *See* PCLOB REPORT, *supra* note 11, at 146 (majority view).

52. *See id.* at 212 (separate statement of Board Member Rachel Brand); *id.* at 217 (separate statement of Board Member Elizabeth Collins Cook). The value of potential future usefulness looms especially large due to the value we place on each American life. *See infra* Part II.C.

B. Bulk Surveillance Costs

It should be unsurprising that program opponents view the costs of bulk surveillance under the 215 program through a different lens than program proponents.[53] Program opponents count as costs infringements on the privacy, autonomy, and free speech rights of those subject to surveillance. Opponents would distinguish the costs incurred when the NSA targets for surveillance persons reasonably suspected of terrorist activity from those incurred when the NSA collects information on virtually everyone.[54] For opponents, collecting information about those with no connection to terrorism represents an unacceptably high cost. For them, having one's data placed in a government database raises the risk of abuse and also affronts privacy and autonomy.[55]

Program supporters take an entirely different approach because they do not view the mere collection of information as even constituting surveillance. For them, a person should not be considered subject to surveillance before an agent has run a query on that person's information in the database, and perhaps not until the person has been identified as connected to that information.[56] Under that view, the vast majority of American citizens have not been subject to surveillance, even though their telephone records have been collected and stored in the NSA's database for at least five years. To program proponents, "merely acquiring an item does not implicate a privacy interest."[57]

Because program proponents do not view the mere collection of data as imposing costs, they assess only the costs to those who are the subject of querying. Because those queries are subject to judicial oversight and limits, program proponents assess those costs as comparatively lower than program opponents.

53. Both tally as costs the resources expended in conducting the surveillance. Any dollar value the Intelligence Community attaches to those resource costs is classified. *July 2013 Hearings*, *supra* note 15, at 27 (statement of Chairman Goodlatte).

54. *See, e.g.*, *id.* at 91, 92 (prepared statements of Jameel Jaffer and Laura W. Murphy, ACLU) (recommending close connection between target of a current investigation and records sought rather than indiscriminate dragnets).

55. *See, e.g.*, Brief for Michael P. Lynch as Amicus Curiae Supporting Plaintiffs at 7–9, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (arguing that mere collection of data violates the data subject's autonomy, whether or not any use is made of the data); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011) (discussing privacy harms that can occur even in the absence of actual surveillance).

56. Government Memorandum in *Clapper*, *supra* note 20, at 25–31; *Admin. White Paper*, *supra* note 29, at 19 (contending that the production of telephony metadata is not a "search" under the Fourth Amendment).

57. *See Clapper*, 959 F. Supp. 2d at 738; *Admin. White Paper*, *supra* note 29, at 15 (contending that any privacy intrusion suffered by the collection of "technical" metadata is "substantially mitigated by the judicially approved restrictions on accessing and disseminating the data").

Even if it only counts as surveillance when an agent runs a query on data or otherwise analyzes it, program opponents tally as program costs the fear of such surveillance that collection creates. According to that view, the storage of their data in NSA's databases facilitates analysis and creates a chilling effect on protected rights of speech and association.[58] That chilling effect, which spreads to people who believe, *even if incorrectly*, that that they are under surveillance, is a cost of the 215 program.

Program supporters regard that formulation as unfair. If people are chilled because of what could happen but is not actually happening, the answer is to stop being chilled rather than hold the program accountable for misplaced fears.[59]

Embedded in the disagreement about the costs of surveillance, then, is a disagreement about trust. Program proponents see no reason to fear collection without analysis and no reason to be chilled about mere collection. Program opponents see no reason to trust that "collection" doesn't necessarily mean "analysis."

C. Costs of Not Conducting Surveillance

When opponents of the 215 program have contemplated scrapping it, they have seen many costs avoided and few, if any, benefits lost. Accordingly, activist groups have pressed courts to enjoin the 215 program and have supported congressional bills to defund it.[60]

Supporters of the 215 program have regarded abandoning it as fraught with peril. According to supporters, if and when another terrorist attack occurs, the American people and their leaders will ask whether the Intelligence Community did everything in its power to prevent the attack.[61] Because each American life is priceless,[62] the reasoning goes, we will tolerate no resource-based excuse for the Intelligence

58. *See infra* notes 101–113.

59. *See, e.g.*, Government Memorandum in *Clapper*, *supra* note 20, at 33–34 (claiming no evidence that NSA analysts have ever accessed or reviewed plaintiffs' metadata and therefore no evidence of a chilling effect).

60. *See supra* note 12 (listing legal challenges); H.R. REP. NO. 113-170, at 29 (2013) (proposing that the funding for the 215 program be discontinued).

61. President Barack Obama, Speech at the Department of Justice on National Security Agency Reforms (Jan. 17, 2014) [hereinafter *Obama January Speech*] (stating that we will ask why the Intelligence Community failed to connect the dots in the event of another 9/11-type attack).

62. *Clapper*, 959 F. Supp. 2d at 755–56 (quoting testimony of Deputy Director Sean Joyce). If American lives are truly of infinite value, that significantly skews the analysis because anything that remotely contributes to saving that infinite value will be worth the cost. More rational analysis is in order. *See* REVIEW GROUP REPORT, *supra* note 11, at 45–48 (noting the need for decisions about surveillance to account for the costs to privacy, freedom, civil liberties and the United States' relationships with other nations).

Community having failed to use *every* method that might have averted an attack.[63] In the wake of another terrorist attack, some contend that Congress will give the NSA powers that make the 215 program seem mild.[64] According to that view, the 215 program represents a moderate effort to avoid a truly intrusive program.

III. DIVERGENT APPROACHES TO THE LEGALITY OF THE 215 PROGRAM

Legal challenges to the 215 program have alleged, among other things, violations of FISA, the Fourth Amendment, and the First Amendment.[65] The Administration has mounted a vigorous defense in court and to the public. The differing legal assessments reflect differing views of the program's value and the risk of abuse it poses.

A. Legality of the 215 Program Under FISA

Program challengers contend that the NSA exceeds its authorization when it operates the 215 program because it does not conform to the statutory text.[66] FISA requires that requests under section 215 include a "statement of facts showing that there are reasonable grounds to believe [the information] sought [is] relevant to an authorized investigation."[67] Most of the litigation has concerned whether the 215 program meets the relevance requirement.[68]

63. *But see supra* notes 21–22 (reporting that the NSA stopped the Internet metadata program in 2011 due to resource and efficacy concerns).

64. *See, e.g.*, *Clapper*, 959 F. Supp. 2d at 757 ("[N]othing is more apt to imperil civil liberties than the success of a terrorist attack on American soil."); Kris, *supra* note 8, at 65 ("If less surveillance leads to a perceived intelligence failure, of course, resulting demands to expand surveillance may cause the pendulum to swing back.").

65. *See, e.g.*, *Clapper*, 959 F. Supp. 2d at 735. They also have raised claims under the Fifth Amendment and other statutes. *See, e.g.*, Plaintiffs' Motion for Partial Summary Judgment that the Telephone Records Program Is Unlawful Under Section 215 of the Patriot Act and the First Amendment at 3 n.1, First Unitarian Church of L.A. v. Nat'l Sec. Agency, No. 13-3287 (N.D. Cal. Feb. 7, 2014) [hereinafter *Motion for Partial Summary Judgment in First Unitarian*] (reserving right to seek summary judgment on Fifth Amendment claim later); Klayman v. Obama, 957 F. Supp. 2d 1, 9 n.7 (D.D.C. 2013) (refusing to address Fifth Amendment claims).

66. In addition to the relevance limit, the pertinent provision states that the FBI will collect the records, but NSA has been collecting the records under the 215 program. *Motion for Partial Summary Judgment in First Unitarian*, *supra* note 65, at 8 n.3. Also, the language seems to refer to records already in existence, but orders under the 215 program have required providers to compile data in real-time and forward it to the providers on an ongoing basis. *See id.* at 13–14; Plaintiff Memorandum in *Clapper*, *supra* note 19, at 14–15, 15 n.12.

67. 50 U.S.C. § 1861a(2)(A) (2006) (for information concerning U.S. persons, the investigation must be "to protect against international terrorism or clandestine intelligence activities").

68. The litigation has raised other issues of statutory compliance. For example, civil

Those opposing the program in court have argued strenuously that the word "relevance" loses all meaning when everything is relevant. They have pressed that "relevance" is a word of limitation, particularly when considered in the context of "an investigation." According to them, the statute requires the NSA to make *some* showing before it may collect the telephony information.[69] To collect all information, in bulk, is to operate outside the statute's purview.

The Administration's legal defense reflects its different perception of the program's function and value. As a purely legal matter, program defenders argue that precedents support interpreting "relevance" broadly enough to encompass the collection of all American's telephony records.[70] Judges have previously approved of grand jury subpoenas, analogous to 215 orders, in contexts where they knew that many of the records that would be disclosed would not be incriminating or pertinent. The 215 program represents a change in scale but not in kind from those earlier cases.[71] In response to the charge that the enormous scale of the 215 program stretches those precedents past their breaking points, program defenders have argued that the program needs virtually *all* of American's telephony data to work.[72]

Program proponents' more expansive view of the benefits of the 215 program undoubtedly inspires a broader view of what counts as relevant information to collect. To them, the NSA needs all of our metadata because the program yields benefits whether a query exonerates or incriminates. Similarly, because the program provides value in that it has the potential to provide information, data that seem irrelevant today may later turn out to be useful. A broad view of relevance is the only way, under this view, to ensure that the 215 program's database of information functions as designed.

Opponents' view that the 215 program yields benefits only when it identifies those culpable, or at least suspected, of terrorist activity

libertarians claim that the 215 program violates the Stored Communications Act ("SCA"), which prohibits the disclosure of telephony records to the government unless pursuant to a set of exceptions that do not list the Section 215 program. Plaintiff's Reply Brief in Support of Their Motion for Preliminary Injunction at 4–6, *Clapper*, 959 F. Supp. 2d 724 [hereinafter ACLU Reply in *Clapper*]; Motion for Partial Summary Judgment in *First Unitarian*, *supra* note 65, at 12–13. The *Clapper* court found that Congress implicitly included Section 215 as an exception to the SCA prohibition. *Clapper*, 959 F. Supp. 2d at 730; *see also supra* note 66.

69. *See* Motion for Partial Summary Judgment in *First Unitarian*, *supra* note 65, at 7–9; PCLOB REPORT, *supra* note 11, at 59–60.

70. Government Memorandum in *Clapper*, *supra* note 20, at 16–22.

71. *See, e.g.*, *Admin. White Paper*, *supra* note 29, at 11; *July 2013 Hearings*, *supra* note 15, at 107 (testimony of Steven G. Bradbury).

72. *See FISC 2013 Opinion, supra* note 27, at 18–22 (agreeing with proponents that "the whole production is relevant to the ongoing investigation out of necessity"); Kris, *supra* note 8, at 20–22 (describing proponents' arguments).

influences their interpretation of relevance. To them, one can know today whether information is relevant by determining if it pertains to a person reasonably suspected of terrorist activity.[73] Under this view, it makes no sense to collect bulk data because that means gathering up a tremendous amount of information about people with no connection to terrorism. To program opponents, doing so is an abuse, as I discuss in Part IV, and a violation of constitutional rights, as I discuss next.

B. Legality of the 215 Program Under the Fourth Amendment

For program defenders, clear Supreme Court precedent establishes that people lack a reasonable expectation of privacy in their metadata. According to them, the NSA conducts no search when it collects information about telephone calls but not their content. Moreover, the 215 program, considered as a whole, meets the constitutional standard of reasonableness. Program challengers, on the other hand, view collection under the bulk surveillance program as exceeding the scope of earlier precedents and violating reasonable expectations of privacy. To them, metadata collection is an unreasonable search unless subject to additional procedural protections and a more limited scope.[74]

1. Is Bulk Collection a Fourth Amendment Search?

The debate over whether the Fourth Amendment regards the collection of metadata as a search has centered on the extent to which *Smith v. Maryland*, a Supreme Court case from 1979, governs.[75] In *Smith*, the Supreme Court distinguished the information the police acquired—telephone numbers the suspect's telephone dialed—from the content of his phone calls.[76] The Court found no expectation of privacy in the former, despite a clear expectation of privacy in the latter under *Katz v. United States*.[77] To program defenders, as well as to the FISC judges who have upheld the 215 program,[78] *Smith* clearly establishes that the Fourth Amendment does not protect the metadata the NSA acquires; its collection does not constitute a search.[79] Further, *Smith* establishes that consumers assume the risk their communications providers will

73. *See, e.g.*, *July 2013 Hearings*, *supra* note 15, at 89 (prepared statements of Jameel Jaffer and Laura W. Murphy, ACLU).

74. Plaintiff's Memorandum of Law in Support of Plaintiffs' Motion for Preliminary Injunction at 23–29, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (arguing that the 215 program is unreasonable either because it is warrantless or because it is indiscriminate).

75. Smith v. Maryland, 442 U.S. 735 (1979).

76. *Id.* at 739.

77. *Id.* (citing Katz v. United States, 389 U.S. 347 (1967)).

78. *See, e.g.*, *FISC 2013 Opinion*, *supra* note 27, at 6.

79. Government Memorandum in *Clapper*, *supra* note 20, at 25–27.

disclose their metadata to the NSA, just as Smith assumed the risk his telephone company would disclose his telephone numbers to the police.[80]

Those challenging the 215 program in court regard the extension of *Smith* to the metadata context as a bridge too far. For them, the lack of Fourth Amendment protection for the telephone numbers dialed by one suspect's landline phone, during a single investigation, over a short period, does not imply the lack of protection for the collection of more extensive and revealing data, obtained continuously for virtually all Americans and stored for five years.[81] Reflecting the view that the program has value only when it independently yields information about terrorist attacks, program challengers disapprove of bulk surveillance as a fishing expedition—exactly what the Fourth Amendment was designed to prohibit.[82]

Because program opponents view collection under the 215 program as falling outside the scope of *Smith*, they look to more recent precedents for guidance. For example, under the Supreme Court's 2012 decision in *United States v. Jones*, five Justices viewed collecting information about a person's movements in public over a prolonged period as violating expectations of privacy under the Fourth Amendment.[83] Opponents view *Jones* as relevant particularly because of the possibility that the 215 program will be extended to other forms of metadata.[84] With that in mind, as well as the Fourth Amendment prohibition against dragnet searches, opponents view collection under the metadata program as constituting a Fourth Amendment search.[85]

80. *See, e.g.*, *FISC 2013 Opinion*, *supra* note 27, at 7–8.

81. *See* ACLU Reply in *Clapper*, *supra* note 68, at 10–11; Klayman v. Obama, 957 F. Supp. 2d 1, 31–37 (D.D.C. 2013) (discussing how modern uses of the cell phone and the ongoing cooperative relationships between providers and the government make *Smith* inapplicable to the 215 program).

82. *See, e.g.*, Plaintiff Memorandum in *Clapper*, *supra* note 19, at 33 (describing searching under the 215 program as a "general warrant," the "most offensive" form of search under the Fourth Amendment); *id.* at 25 (describing the program as a "startling intrusion" that is a "blanket invasion of Plaintiffs' – and every Americans' – right to privacy").

83. *Klayman*, 957 F. Supp. 2d at 31 (citing United States v. Jones, 132 S. Ct. 945 (2012)).

84. *See, e.g.*, ACLU Reply in *Clapper*, *supra* note 68, at 10 (noting that Government's theory would permit it to acquire as metadata: "email metadata, internet-usage history, internet-chat records, financial records, credit-card records, 'and even portions of medical records'"); Brief of Amicus Curiae Nat'l Rifle Assoc. of Am. Supporting Plaintiff at 14, 17–18, ACLU v. Clapper, 959 F. Supp.2d 724 (S.D.N.Y. 2013) [hereinafter *NRA Amicus Brief*] (arguing that the government's statutory reading would permit it to seek all records of gun purchases, credit card transactions, and website traffic); Smith v. Obama, 2014 WL 2506421, at *3 (D. Idaho June 3, 2014) (raising legal concerns about the ability to discern location from the data collected, including "trunk identifier").

85. *See, e.g.*, *July 2013 Hearings*, *supra* note 15, at 84 (prepared statement of Jameel Jaffer and Laura W. Murphy, American Civil Liberties Union) ("The Fourth Amendment is triggered by the *collection* of information, not simply by the querying of it."); ACLU Reply in

If the NSA is not tracking location data, as it claims,[86] then *Jones* does not clearly apply.[87] Arguing that new Fourth Amendment privacy rights do not exist until the Supreme Court explicitly affirms them, program supporters assert the right to rely on established precedents.[88] At least some program opponents, by contrast, have encouraged courts to engage in a normative analysis that recognizes the need to adapt Fourth Amendment rights to new technologies.[89]

2. Fourth Amendment Reasonableness

Whether or not collection itself counts as a search under the Fourth Amendment, defenders contend that the program satisfies the Fourth Amendment because it is constitutionally reasonable.[90] To defenders, the 215 program operates reasonably because NSA agents conduct queries subject to oversight by the FISC, Congress, the Department of Justice, and other elements in the Intelligence Community.[91] FISC primary orders limit the NSA's queries in terms of the RAS standard and place other significant limits on the program's operations.[92] Internal reviews, often as part of the renewal process, have yielded disclosures of problems, enhanced oversight, and reform.[93] To program supporters, those mechanisms limit the intrusion, if any, on privacy interests, while the overarching value of the program weighs strongly on the side of reasonableness.[94]

Program challengers question the adequacy of current oversight

Clapper, *supra* note 68, at 10–12.

86. *See Smith*, 2014 WL 2506421, at *3 ("The NSA denies that it is tracking location.").

87. In addition, only the *Jones* concurrences considered tracking without installation of a GPS tracking device, which is what NSA tracking would be.

88. *See Smith*, 2014 WL 2506421, at *4 ("But *Smith* [*v. Maryland*] was not yet overruled and it continues – along with the Circuit decisions discussed above – to bind this Court.")

89. *See, e.g.*, *Klayman*, 957 F. Supp. 2d at 37 n.60 (explaining that should people lack a subjective expectation of privacy in their metadata, a normative inquiry would be proper). *Cf.* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 745-46 (2011) (recommending that courts addressing historical cell site location data adopt the Sixth Circuit's normative approach to finding reasonable expectations of privacy in stored email).

90. *See, e.g.*, ADMIN. WHITE PAPER, *supra* note 29, at 15 (arguing that although the Fourth Amendment does not apply, its reasonableness requirement is met by access and dissemination limits).

91. Government Memorandum in *Clapper*, *supra* note 20, at 31-33; *Admin. White Paper*, *supra* note 29, at 4-5.

92. See *FISC Primary Order*, *supra* note 23.

93. Proponents also cite to Congress' reauthorization of the program as further evidence of its reasonableness. *See Admin. White Paper*, *supra* note 29, at 17–19. Opponents question whether legislators had adequate knowledge of the program's operation. *See, e.g.*, *July 2013 Hearings*, *supra* note 15, at 84. *See also* Kris, *supra* note 8, at 43–58 (discussing debate over congressional briefings).

94. *See, e.g.*, *Admin. White Paper*, *supra* note 29, at 15.

mechanisms to minimize harms.[95] First, although the FISC has implemented the RAS standard in its primary orders, those orders are not codified in the statute and are therefore subject to change. Second, a FISC opinion made public after the Snowden disclosures revealed that the NSA had made a large number of NSA queries not meeting the RAS standard.[96] The FISC opinion found not only numerous compliance faults but also that the government had materially misrepresented its compliance over a period of years.[97] Third, opponents have questioned how well Congress has discharged its oversight responsibilities, as well as reliance on the NSA to disclose its own compliance problems. Finally, although the NSA has emphasized how few seeds there have been, an exceptionally large number of people's records have come under scrutiny as a result of contact-chaining.[98] After records are selected as seed queries and through hops, they are no longer subject to the RAS restrictions on analysis.[99]

To sum up, program supporters find reasonableness in how the 215 program is designed, structured, and approved. Opponents find unreasonable how the 215 program operates; it unnecessarily and indiscriminately collects much more sensitive information than it needs and subjects that information to analysis and risk of abuse.[100] As I discuss further in Part IV, proponents claim that the system works—when problems are identified, they are remedied. Opponents argue that the problems that have been identified may well persist, and, worse, they may be only the tip of the iceberg.

95. *See supra* Part II for a discussion of the different views on the 215 program's effectiveness, or value, which provides the other part of the reasonableness balance.

96. *See In re* Production of Tangible Things from [Redacted] at 11, No. BR 08-13 (FISA Ct. Mar. 2, 2009) [hereinafter *FISC 2009 Opinion*] (Walton, J.) (complaining that the minimization procedures had been "so frequently and systemically violated that it can fairly be said that this critical element of overall [215 program] has never functioned effectively").

97. *Id.* at 6–9.

98. In a telling example of divergent views, ACLU and government lawyers have made radically different estimates of how many phone numbers the NSA acquires in a typical three-hop analysis, while assuming the same number of average contacts per person (forty). The government estimated that the NSA analysts would collect 64,000 phone numbers while the ACLU estimated that they would collect 2.5 million because analysts would collect the calling records, not just the phone numbers, of those within three hops of the seed. The correct approach remains unclear. *See* ACLU Reply in *Clapper*, *supra* note 68, at 14 n.10; Government Memorandum in *Clapper*, *supra* note 20, at 8 n.3 ("The correct number of records, using Plaintiffs' hypothetical example of forty contacts per person, [is] 65,640, not over two million.").

99. *See supra* notes 35–40 (describing data in corporate store); Katherine J. Strandburg, *Membership Lists, Metadata, and Freedom of Association's Specificity Requirement*, 10 J.L. & POL'Y FOR INFO. SOC'Y 327, 355–56, 362–64 (2014) (raising concerns about the "corporate store").

100. *See supra* note 74; ACLU Reply in *Clapper*, *supra* note 68, at 10–15.

C. Legality of the 215 Program Under the First Amendment

Those who oppose the 215 program view it as infringing on First Amendment rights to speak free of government censorship, to associate with others without being tracked, and to a free and robust press.[101] Studies have shown that even a small amount of metadata can reveal a person's health conditions, religious preferences, philosophical commitments, and political views.[102] Press contacts reveal journalists' sources and potential whistleblowers may refrain from seeking counsel if they believe the government is logging their communication partners.[103] An impressive array of amici supported challenges to the 215 program by reporting that they felt chilled by the knowledge that the NSA was collecting their metadata.[104]

As discussed, supporters have questioned whether people have cause to feel any chill at all.[105] According to a district court judge who upheld the program, if people feel chilled, they are overreacting to irrational fears that intelligence agents will stray well beyond their mandate of fighting terrorism.[106]

For program opponents, past intelligence abuses make their fears entirely rational.[107] In 1976, the Church Committee, whose report provided the impetus for FISA, described how intelligence agencies had developed detailed profiles of tens of thousands of activists, writers, and politicians whom the government viewed as potentially subversive but who were engaged in no illegal behavior.[108] The Church Committee's

101. *See, e.g.*, Motion for Partial Summary Judgment in *First Unitarian*, *supra* note 66, at 17–25 (discussing the 215 program's chilling effect and its violation of First Amendment rights); ACLU Reply in *Clapper*, *supra* note 68, at 15–20; Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013) (describing the chilling effect of surveillance).

102. Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata,* WEB POLICY (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.

103. *See* Strandburg, *supra* note 99, at 337–38, 362 (discussing how various group members feel chilled by the 215 program, particularly members of minority groups).

104. *See, e.g.*, *NRA Amicus Brief, supra* note 84; Brief of Amicus Curiae Pen Am. Ctr. in Support of Plaintiff's Motion for a Preliminary Injunction and in Opposition to Defendant's Motion to Dismiss, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

105. *See supra* note 59; Government Memorandum in *Clapper*, *supra* note 20, at 1–2, 13–14, 33–36.

106. *See, e.g.*, *Clapper*, 959 F. Supp. 2d at 754 (dismissing the ACLU's claim of a chilling effect as arising from a "speculative fear"); *id.* at 751, 751 n.17 (dismissing the ACLU's "parade of horribles" and crediting the NSA's denial that it engages in pattern analysis).

107. *See, e.g.*, *July 2013 Hearings*, *supra* note 15, at 110–11 (testimony of Kate Martin, Center for National Security Studies) (describing as chief concern that government will use surveillance to chill political dissent and challenge political opponents, as has happened "too many times" in history); *id.* at 84 (testimony of Jameel Jaffer, ACLU) (referring to the Church Committee findings of FBI abuse as reasons to be concerned about NSA surveillance).

108. *See* REVIEW GROUP REPORT, *supra* note 11, at 55–68; Brief for Former Members

report concluded that governments naturally tend to abuse their powers, secretly expanding their intelligence activities "beyond their initial scope" to "generate ever-increasing demands for new data."[109] In 1972, the Supreme Court recognized that governments will naturally see as threats anybody who opposes them.[110] Program opponents extrapolate from history, current abuses, and a lack of oversight to assert that the NSA is building profiles of perceived opponents. A former Department of Justice official involved in NSA oversight has countered that new restrictions and oversight mechanisms that were previously lacking ensure that we will not return to the abuses of the past.[111]

In litigation, the conflict has crystallized over whether the NSA has matched names to the telephony metadata to form detailed individual profiles. Program advocates have maintained that the NSA does not put names together with the unique identification numbers unless and until it has good cause to do so.[112] Opponents respond that it is as easy to associate a unique identifier with a name as it is to look up a number in the telephone book[113] and that proponents have been obscuring that issue.[114]

of the Church Comm. and Law Professors as Amici Curiae Supporting Plaintiff, *Clapper*, 959 F. Supp. 2d 724 (describing how the 215 program conflicts with Congress's efforts to prevent more intelligence abuses of the type revealed in the Church Committee report) (I signed onto this brief).

109. REVIEW GROUP REPORT, *supra* note 11, at 58 (quoting S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, FINAL REPORT OF THE UNITED STATES SENATE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES OF THE UNITED STATES SENATE, S. REP. NO. 94-755, at v, vii, 1, 3 (1976).

110. United States v. U.S. Dist. Ct. (*Keith*), 407 U.S. 297, 313 (1972) (recognizing "greater jeopardy to constitutionally protected speech" in "[n]ational security cases"); *see also id.* at 314 ("The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.").

111. *See* Todd Hinnen, former Acting Assistant Attorney for Nat'l Sec. at the Dep't of Justice, Remarks at the Silicon Valley Flatiron Symposium: New Frontiers of Privacy Harm—Panel One: Is Government Surveillance Harmful (Jan. 7, 2014), *available at* https://www.youtube.com/watch?v=H6ni98L2vxk&index=1&list=PLTAvIPZGMUXNfrXy3VzpDtIPlyJjCjyKt (remarks begin at 2:07:30) (explaining how extensive new safeguards make abuses of the past much less likely now).

112. Government Memorandum in *Clapper*, *supra* note 20, at 2, 16, 28.

113. ACLU Reply in Clapper, *supra* note 68, at 14–15 (citing Felten Declaration); *see also* ADMIN. WHITE PAPER, *supra* note 29, at 4 (noting that the FBI may rely on publicly available information to identify the subscribers associated with telephone numbers).

114. *See, e.g.,* Julian Sanchez, *A Reply to Epstein & Pilon on NSA's Metadata Program*, CATO INST. (June 16, 2013), http://www.cato.org/blog/reply-epstein-pilon-nsas-metadata-program (arguing that it is trivially easy for NSA to attach names to metadata records using publically available sources and that those who argue otherwise are misleading the public).

IV. DIVERGENT APPROACHES TO WHAT CONSTITUTES ABUSE

A. Program Proponents Define Abuse Narrowly

Proponents argue that there have been few, if any, abuses of the 215 program. For them, an abuse occurs only when an agent intentionally or in bad faith engages in unlawful activities.[115] Under that definition, only those few rogue agents who misused their surveillance authorities to find out about former girlfriends count as abusers, but none of those agents used 215 program authorities.[116] Proponents have reported seeing no comparable evidence of intentional abuses under the 215 program.[117]

B. Program Opponents Define Abuse Broadly

1. Not Following Procedures as an Abuse

A 2009 opinion by FISC Judge Reggie Walton revealed a large number of instances in which agents conducted queries that did not conform to the requirements established in the FISC orders.[118] For example, agents used seed identifiers to query terms that were on an "alert list" of persons of interest but that had not satisfied the RAS standard.[119] In his opinion, which remained classified until after the Snowden disclosures, Judge Walton identified several ways in which the NSA had failed to comply with its own minimization procedures, improperly trained agents, and failed to segregate information.[120]

Because members of the NSA had themselves reported the compliance problems, program proponents said that the system worked.[121] They described irregularities as variously the result of human error and the technological complexity of the systems upon which the 215 program relies.[122] Program proponents cited to the disclosures as evidence that problems do see the light of day and get fixed; they noted that no reports of new problems indicate that the agency has fixed its

115. Kris, *supra* note 8, at 17 (quoting the Director of National Intelligence as stating, in a July 2013 letter, "there have been no findings of any intentional or bad-faith violations" of the section 215 program).

116. Siobhan Gorman, *NSA Officers Spy on Love Interests*, WASH. WIRE (Aug. 23, 2013), http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/.

117. *Id.*

118. *FISC 2009 Opinion*, *supra* note 96.

119. *Id.* at 4–5, 15.

120. *Id.* at 9–11, 13–14; *see also* Kris, *supra* note 8, at 15–17 (detailing compliance issues with metadata program).

121. *See* Kris, *supra* note 8, at 15–17.

122. Government Memorandum in *Clapper*, *supra* note 20, at 9, 10 n.5; Kris, *supra* note 8, at 15–17.

prior problems by using new protocols and enhancing supervision.[123]

Program opponents have regarded the errors just described as abuses. It took the NSA several years to report problems to the FISC, during which the problems were ongoing. And while Judge Walton's increased oversight indicates that he did not see himself as a "rubber stamp," he permitted the program to continue, albeit with reforms.[124] Program opponents find it difficult to trust that there have been no subsequent problems because the system relies on self-reporting. Perhaps the NSA has merely chosen not to report abuses. Misleading and arguably untruthful statements by intelligence officials[125] add fuel to the fire of opponents' distrust.

2. Mission Creep as an Abuse

Stories have surfaced indicating that other agencies have been clamoring to get access to the bulk data collected under the 215 program and that some may have been successful.[126] To program opponents, loose sharing of collected data illustrates dangerous mission creep. While our representatives weigh the benefits from protecting against a terrorist attack quite high, they do not place the same weight on obtaining more efficient law enforcement investigations. Program opponents view it as an abuse to have citizens sacrifice their civil liberties for better law enforcement when they believe that they are doing so only to combat terrorism.

Program proponents cite to the limits the FISC has placed on sharing information with the FBI and other intelligence agencies.[127] While FISA permits disseminating information analyzed under the 215 program to understand foreign intelligence information,[128] FISC primary

123. *Cf. July 2013 Hearings*, *supra* note 15, at 72 (statement of Stewart A. Baker, former NSA General Counsel) ("But if in fact abuses were common, we'd know it by now.").

124. The FISC further restricted the 215 program for some period after its decision. Kris, *supra* note 8, at 17.

125. *See, e.g.*, *July 2013 Hearings*, *supra* note 15, at 3–4 (statement of Representative Conyers) ("We know Director Clapper's misstatements and others. National Security Agency Director General Keith Alexander had to make retractions.").

126. *See, e.g.*, Kris, *supra* note 8, at 14–15 n.58 (discussing disclosure by NSA that unminimized metadata query results had been made available to other intelligence agencies); Brian Fung, *The NSA Is Giving Your Phone Records to the DEA and the DEA Is Covering It Up*, WASH. POST (Apr. 5, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/05/the-nsa-is-giving-your-phone-records-to-the-dea-and-the-dea-is-covering-it-up/ (acknowledging uncertainty about whether shared data came from the 215 program).

127. *See* Government Memorandum in *Clapper*, *supra* note 20 at 9 (describing limits on NSA's disclosures); *FISC Primary Order*, *supra* note 23, at 13–14 (limiting NSA dissemination).

128. *See* 50 U.S.C. § 1861(g)(2)(B) (2006).

orders permit information about U.S. persons to be shared only to understand counterterrorism information or assess its importance.[129] Counterterrorism is a much narrower category than foreign intelligence.[130] Proponents would argue that sharing outside those limits results either from unintentional mistakes or from compliance problems that generally come to light through effective oversight.

3. Does Government Possession of Data Constitute an Abuse?

To program opponents, as previously mentioned, there are plenty of reasons to be concerned about the collection of data independent of the Fourth Amendment status of the collection. Personal data in a government-controlled database can be viewed as a honeypot that attracts attention.[131] Edward Snowden's ability to obtain so much ostensibly secret information has fueled concerns about the security of the NSA's own stored data. Insecure data is vulnerable to attack by outsiders, foreign or domestic—malicious hackers and identity thieves. It is similarly vulnerable to insiders, to further their own personal schemes or to use the information for such prohibited purposes as discrimination, harassment, and blackmail.[132]

4. What to Assume About Abuses in the Absence of Information About Them

In the absence of definitive information, those who oppose the program assume that abuses are occurring. They contend that the public's knowledge remains incomplete and it is quite likely that further disclosure would reveal more problems.[133] Program proponents assume the opposite; in the absence of evidence of abuses, people have no reason to be concerned.[134]

129. *FISC Primary Order*, *supra* note 23, at 13.

130. *See supra* note 41.

131. *See* GREG CONTI, GOOGLING SECURITY: HOW MUCH DOES GOOGLE KNOW ABOUT YOU? 19, 20 (2009) (describing the threats to the mass of consumer data Google collects, many of which do not come from Google itself).

132. *Cf. Policy Directive 28*, *supra* note 41 (prohibiting the use of collected data to suppress or burden "criticism or dissent" or to disadvantage people based on their "ethnicity, race, gender, sexual orientation, or religion").

133. For example, disclosures have been limited about the extent of location data and internet metadata collected, where that information is stored now, whether it is merged with telephony metadata in some way, and, if so, whether such information may be used as seeds for querying. Information remains scant about corporate store information and how it is analyzed. Of course, the public remains in the dark about still-secret programs that may well interact with metadata collected under the 215 program.

134. *See Obama January Speech*, *supra* note 61 (suggesting that, in May 2013, President

CONCLUSION

As it stands, the current disjunction inhibits members of the public from meaningfully engaging in the debate over the proper scope of national security surveillance.[135] Those not directly involved, but trying to keep up, hear two non-reconcilable stories. They feel pressure to choose allegiance to one side or the other; they cannot accept both at the same time and a nuanced position seems unavailable. If the terms of the debate were more joined, people could take positions reflecting more than an untutored impulse either to trust or distrust the government.

In the short to medium term, changes to the 215 program could well decrease some of the tension between the two sides. As discussed earlier, President Obama instituted some changes and announced the consideration of others.[136] Following the recommendations of the PCLOB and the President's Review Group, legislation pending in Congress could place further limits on the program, increase transparency, and add an adversary to the mix.[137] Appellate and even Supreme Court review of pending cases should resolve some of the legal questions more definitively.

But the lack of a common basis for describing costs and benefits, the legal framework, and what counts as abuses will persist as we continue to face questions about the proper scope of national security surveillance. That means that the two sides may well miss opportunities for collaboration because of the bad feelings engendered by not speaking the same language.[138] My sense is that proponents of national security surveillance feel unfairly accused of operating in bad faith and want more credit for their efforts to act lawfully. At the same time, opponents of such surveillance resent the resistance to obtaining surveillance disclosures and being accused of having unfounded fears. Turning down the heat on the discussion could yield greater opportunities for agreement and for greater participation by the public in the design of a workable

Obama was contemplating how to increase disclosures about NSA surveillance to improve public understanding).

135. *See* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE 23–24 (2014) (quoting Edward Snowden as claiming to be motivated solely by a desire to raise public awareness and spur debate over surveillance practices).

136. *See supra* note 31; *Obama January Speech*, *supra* note 61.

137. *See*, *e.g.*, USA FREEDOM Act, H.R. 3361, 113th Cong. (2014); *see also* Kris, *supra* note 8, at 62–67 (proposing ways to improve transparency and public understanding on intelligence activities); Lederman, *supra* note 10 (criticizing current FISC procedures for not being adversarial and strongly commending Kris' proposals).

138. I am not claiming that collaboration or compromise is always available. But I think that opportunities may be missed when a party feels that she is acting in good faith without recognition of that.

system. Understanding what others mean by the terms they use is a crucial step forward.