2015

Beyond the Fourth Amendment: Additional Constitutional Guarantees That Mass Surveillance Violates

Nadine Strossen
New York Law School, nadine.strossen@nyls.edu

Recommended Citation
63 Drake L. Rev. 1143 (2015)

BEYOND THE FOURTH AMENDMENT: ADDITIONAL CONSTITUTIONAL GUARANTEES THAT MASS SURVEILLANCE VIOLATES

*Nadine Strossen**

ABSTRACT

The ongoing dragnet communications surveillance programs raise multiple statutory and constitutional problems. Each problem alone, and even more so the whole combination, provides a serious ground at least for vastly curbing such programs, if not ending them. This Article reviews constitutional challenges to these programs to evaluate the likely success of current and future litigants.

TABLE OF CONTENTS

Privacy concerns are a sobering and important topic. As Sun Microsystems CEO Scott McNealy famously said, way back in 1999: "You have zero privacy anyway. Get over it."[1] Likewise, for the constitutional law dimension in 1983 (sixteen years earlier), Georgetown Law Professor Silas Wasserstrom,[2] Laura Donohue's colleague, wrote the article—the title of

* John Marshall Harlan II Professor of Law; Former President, ACLU (1991–2008). The Author was delighted to return to Drake's Constitutional Law Center in connection with this Article. This was her third appearance at the annual Constitutional Law Symposium, and it was an honor to share the podium with the distinguished co-panelists of *Eyes and Ears Everywhere? Privacy in an Age of Government and Technological Intrusion*. *See* DRAKE LAW, *Constitutional Law Symposium*, http://www.law.drake.edu/clinicscenters/conlaw/?pageid=conlawsymposium (last visited Aug. 25, 2015).

1. Polly Sprenger, *Sun on Privacy: 'Get Over It,'* WIRED (Jan. 1, 1999), http://archive.wired.com/politics/law/news/1999/01/17538.

2. *See Our Faculty*, GEORGETOWN LAW, https://www.law.georgetown.edu/faculty/wasserstrom-silas-j.cfm (last visited Aug. 25, 2015). Professor Wasserstrom is a colleague of one of the Author's co-panelists at Drake's 2015 Constitutional Law

which tracked that of a classic sci-fi film[3]—*The Incredible Shrinking Fourth Amendment*.[4] Unfortunately, while the film was science fiction, the article was not.

Worse yet, in the decades since then, the Supreme Court has continued to shrink the Fourth Amendment in crucial ways,[5] although there have been some bright spots and some basis for hoping that the Court might provide increased protection for digital privacy.[6] Because Laura Donohue is a leading Fourth Amendment scholar who is sharing her insights on point for this Symposium,[7] the best use of this Article is to focus on other constitutional guarantees that are violated by the government's mass

---

Symposium, Laura Donahue. *See Constitutional Law Symposium*, DRAKE LAW, http://www.law.drake.edu/clinicscenters/conlaw/?pageid=conlawsymposium (last visited Aug. 25, 2015).

3. *See* THE INCREDIBLE SHRINKING MAN (Universal Studios 1957). *The Incredible Shrinking Man* is a 1957 science fiction film directed by Jack Arnold and adapted for the screen by Richard Matheson from his novel *The Shrinking Man*. The film won the first Hugo Award for Best Dramatic Presentation presented in 1958 by the World Science Fiction Convention. In 2009, it was named to the National Film Registry by the Library of Congress for being culturally, historically, or aesthetically significant and will be preserved for all time.

4. *See generally* Silas J. Wasserstrom, *The Incredible Shrinking Fourth Amendment*, 21 AM. CRIM. L. REV. 257 (1984).

5. *See, e.g.*, Thomas P. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303, 305 (2010) (discussing the "Third Party Exception" to the Fourth Amendment's warrant requirement); Gaby Ghoshray, *Doctrinal Stress or in Need of a Face Lift: Examining the Difficulty in Warrantless Searches of Smartphones Under the Fourth Amendment's Original Intent*, 33 WHITTIER L. REV. 571, 610 (2012) (noting a judicial trend of shrinking citizens' fundamental liberties in favor of governmental administrative interests). For a discussion on the historical foundations of the Fourth Amendment's warrant requirement see, John M.A. DiPippa, *Is the Fourth Amendment Obsolete?—Restating the Fourth Amendment in Functional Terms*, 22 GONZ. L. REV. 483, 503–14 (1988).

6. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2494–95 (2014) (recognizing a privacy interest in modern cell phones and holding warrantless searches of cell phones incident to arrest are unconstitutional under the Fourth Amendment); United States v. Jones, 132 S. Ct. 945, 954 (2012) (holding the attachment of a GPS device by law enforcement to a car was an unreasonable search under Fourth Amendment); *see also*, Andrew Pincus, *Evolving Technology and the Fourth Amendment: Implications of* Riley v. California, 2014 CATO SUP. CT. REV. 307, 308 (2014) (suggesting the *Riley* standard will become a "bulwark for protecting individuals' privacy against the threat of unjustified government intrusion").

7. *See generally* Laura K. Donohue, *The Dawn of Social Intelligence (SOCINT)*, 63 DRAKE L. REV. 1061 (2015).

communications surveillance since 9/11.

This surveillance has been challenged on such other constitutional grounds by a number of organizations and individuals, including the American Civil Liberties Union (ACLU)[8] and the Electronic Frontier Foundation (EFF).[9] These lawsuits, which are still wending their way through the courts,[10] have raised multiple claims. Plaintiffs in these lawsuits maintain that the surveillance violates the statutes on which the government relies: namely, the Patriot Act section 215,[11] for the indiscriminate surveillance of metadata from phone calls of everyone in the U.S.[12] and the FISA Amendments Act (FAA) section 702,[13] for the incidental surveillance of the content from Americans' phone calls while targeting phone calls from non-Americans.[14] The plaintiffs further claim that the surveillance violates the Fourth Amendment, which directly constrains the government's power to invade U.S. citizens' privacy.[15]

In addition, the litigants press claims that this dragnet communication surveillance infringes several other constitutional guarantees:

1) The First Amendment freedoms of speech, press, association, and religion;[16]

---

8. *See Privacy and Surveillance*, ACLU, https://www.aclu.org/issues/national-security/privacy-and-surveillance (last visited Aug. 23, 2015).

9. *Privacy*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/privacy (last visited Aug. 23, 2015).

10. *See, e.g.*, Charles Savage, *A.C.L.U. Asks Court to Stop Part of N.S.A.'s Bulk Phone Data Collection*, N.Y. TIMES (July 14, 2015), http://www.nytimes.com/2015/07/15/us/politics/aclu-sues-to-stop-part-of-nsas-bulk-phone-data-collection.html?_r=0; *Jewel v. NSA*, ELEC. FRONTIER FOUND., https://www.eff.org/cases/jewel (last visited Sept. 23, 2015).

11. 50 U.S.C. § 1861 (2012).

12. *See* ACLU v. Clapper, 785 F.3d 787, 818 (2d Cir. 2015).

13. 50 U.S.C. § 1881a (2012).

14. *See* Brief of Appellant American Civil Liberties Union, American Civil Liberties Union of Oregon, and Electronic Frontier Foundation in Support of Defendant-Appellant at 6, United States v. Mohamud, No. 3:10-cr-00475-KI-1 (9th Cir. Jun. 3, 2015) [hereinafter EFF Brief].

15. *See id.* at 12; Complaint for Constitutional and Statutory Violations, Seeking Declaratory and Injunctive Relief at 14, First Unitarian Church of L.A. v. NSA, No. 3:13-CV-03287 JSW (N.D. Cal. July 16, 2013) [hereinafter Unitarian Church Complaint].

16. *See, e.g.*, Complaint for Constitutional and Statutory Violations, Seeking Damages, Declaratory, and Injunctive Relief at 22–24, Jewel v. United States, 965 F. Supp. 2d 1090 (N.D. Cal. 2013) (No. C 08–04373 JSW, No. C 07–00693 JSW); Complaint for Declaratory and Injunctive Relief at 6, ACLU v. NSA, 438 F. Supp. 2d 754 (E.D.

2) The Second Amendment's right to bear arms;[17]

3) The Fifth Amendment's substantive and procedural due process rights;[18]

4) The Sixth Amendment's right to counsel;[19] and

5) Article III's ban on federal courts issuing advisory opinions.[20]

So far, there are almost no judicial rulings on any of these claims, in part because the courts have unfortunately accepted the government's non-justiciability arguments.[21] Courts should not reach the merits of these other constitutional issues, but for a very different reason: because the bulk surveillance should be invalidated directly on statutory or Fourth Amendment grounds. Indeed, in *ACLU v. Clapper,* the Second Circuit recently held that the bulk domestic phone metadata program was not authorized by Section 215 as the government argued, and hence found it was unnecessary to resolve the First and Fourth Amendment issues that the plaintiffs had also raised.[22]

Nonetheless, it is important to understand that this bulk surveillance also imperils multiple constitutional guarantees, thus magnifying its harm to individual rights and our constitutional order, and underscoring that, we must rein it in through litigation or legislation.

Mich. 2006) (No. 06-CV-10204); Complaint for Declaratory and Injunctive Relief at ¶ 41, Muslim Cmty. Ass'n of Ann Arbor v. Ashcroft, No. 03-72913, 2003 WL 23851817 (E.D. Mich. July 30, 2003).

17. *See* Declaration of Gene Hoffman, Jr. for Calguns Foundation, Inc. in Support of Plaintiffs' Motion for Partial Summary Judgment at 2–3, Frist Unitarian Church of L.A. v. NSA, No. 3:13-CV-03287-JSW (Feb. 7, 2014).

18. Unitarian Church Complaint, *supra* note 15, at 15–17.

19. *See* Brief Amicus Curiae of The National Association of Criminal Defense Lawyers at 1–4, Frist Unitarian Church of Los Angeles v. NSA, No. 3:13-CV-03287-JSW (Nov. 18, 2013).

20. United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *9 (D. Or. Jun. 24, 2014).

21. *See, e.g.*, Amnesty Int'l USA v. Clapper, 133 S. Ct. 1138, 1153–55 (2013) (dismissing Plaintiff's claim for lack of standing); ACLU v. Nat'l Sec., 493 F. Supp. 3d 644, 720 (6th Cir. 2007) (dismissing Plaintiff's claim for lack of standing); Jewel v. Nat'l Sec. Agency, 965 F. Supp. 2d 1090, 1112 (N.D. Ca. 2013) (dismissing Plaintiff's claims on the basis of state secrets privilege).

22. ACLU v. Clapper, 785 F.3d 787, 826 (2d Cir. 2015).

I. FIRST AMENDMENT

This Article begins with the vital First Amendment freedoms at stake. The Supreme Court has long recognized that government investigative activities, including communications surveillance, endanger these freedoms.[23] This was the basis for the Court's landmark 1958 ruling in *NAACP v. Alabama*, which struck down a state order for the NAACP to disclose its membership lists.[24] As the Court explained:

> This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. . . . Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.[25]

Justice Sotomayor recently summarized this longstanding concern as follows: "Awareness that the government may be watching chills associational and expressive freedoms."[26] Even more recently, when discussing the indiscriminate Section 215 phone surveillance, President Obama acknowledged that privacy in communications is an essential aspect of our First Amendment rights and expectations.[27]

Notably, the Court has expressly affirmed the foregoing First Amendment principles in the context presented by the bulk phone surveillance programs: electronic communications surveillance for national security purposes.[28] In a 1972 case, which invalidated such surveillance when carried out without individualized probable cause warrants,[29] the Court

---

23. *See, e.g.*, NAACP v. Ala. ex rel. Patterson, 357 U.S. 449, 466 (1958).

24. *Id.*

25. *Id.* at 462; *accord* Watkins v. United States, 354 U.S. 178, 197 (1957) (invalidating a conviction for refusal to divulge sensitive associational information, noting that "forced revelations concern matters that are unorthodox, unpopular, or even hateful to the general public . . . [and] may be disastrous [for the witness]"); *see also* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (stating that the First Amendment protects the speaker against compelled disclosure of identity); Tally v. California, 362 U.S. 60, 65 (1960) (same).

26. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

27. Josh Gernstein, *Obama Plans New Limits on NSA Surveillance*, POLITICO (Dec. 5, 2013), http://www.politico.com/politico44/2013/12/obama-plans-new-limits-on-nsa-surveillance-178986.html.

28. *See* United States v. U.S. Dist. Court for the E.D. of Mich., 407 U.S. 297, 313–14 (1972).

29. *Id.* at 323–24.

detailed why warrantless national security wiretapping undermines both First and Fourth Amendment rights:

> National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. . . . The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." . . .
>
> 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.[30]

Although this case involved domestic intelligence gathering,[31] the D.C. Circuit Court of Appeals reached the same conclusion in a case involving foreign intelligence; it ruled in order to safeguard both First and Fourth Amendment rights, that a warrant was required for the surveillance of an organization.[32]

The Supreme Court has held that when government investigative activities implicate individuals' expressive activities, the government must comply with especially strict Fourth Amendment standards—to safeguard First Amendment rights.[33] In these situations, the Court has applied the Fourth Amendment probable cause and warrant requirements with the goal of "leav[ing] as little as possible to the discretion or whim of the officer in the field."[34]

Moreover, when the government's investigative activity substantially

---

30. *Id.* at 313–14.

31. *Id.* at 299 (noting the case involved a "delicate question of the President's power . . . to authorize electronic surveillance in internal security matters without prior judicial approval").

32. *See* Zweibon v. Mitchell, 516 F.2d 594, 633–34, 669 (D.C. Cir. 1975).

33. Zurcher v. Stanford Daily, 436 U.S. 547, 564 (1978) ("Where the materials sought to be seized may be protected by the First Amendment, the requirements of the Fourth Amendment must be applied with 'scrupulous exactitude.'" (quoting Stanford v. Texas, 379 U.S. 476, 485 (1965))).

34. *Id.* at 564.

burdens First Amendment freedoms, the First Amendment provides independent protection that is distinct from, and in some respects greater than, what the Fourth Amendment provides.[35] An investigative measure that substantially burdens First Amendment rights is subject to "exacting" or "strict" scrutiny;[36] the measure is presumed unconstitutional and will be struck down unless the government can show that it is the least restrictive means for pursuing a compelling state interest.[37]

The Second Circuit recognized the independence of First and Fourth Amendment claims in a case involving border searches of American Muslims who were returning to the U.S. from a Muslim conference in Canada.[38] Even though the court had rejected the plaintiffs' Fourth Amendment claims, it independently analyzed their First Amendment claims, which arose from the very same searches, explaining:

> Our conclusion that the searches constituted a significant or substantial burden on plaintiffs' First Amendment associational rights is unaltered by our holding [rejecting their claims] under the Fourth Amendment.... [T]he First Amendment requires a different analysis,

---

35. *See* N.Y. Times Co. v. Gonzales, 459 F.3d 160, 167–68 (2d Cir. 2006) (holding government subpoenas of records of third parties detailing the work of reporters are covered by the same protections under the First Amendment as the reporters themselves and their personal records); *see also* Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n of N.Y. Harbor, 667 F. 2d 267, 269 (2d Cir. 1981) (holding union payroll records were protected from discovery by the government under the First Amendment as the records "play[ed] an integral part in facilitating [the] association's normal arrangements for obtaining members or contributions").

36. *See, e.g.*, Nat'l Commodity & Barter Ass'n v. Archer, 31 F.3d 1521, 1531 n. 4 (10th Cir. 1994) (noting seizure of an organization's membership information requires the use of strict scrutiny standard of review); *In re* Grand Jury Proceedings, 776 F.2d 1099, 1102–03 (2d Cir. 1985) (holding a grand jury subpoena seeking to elicit testimony involving information invoking the right to freedom of association under the First Amendment is subject to strict scrutiny); Clark v. Library of Cong., 750 F.2d 89, 94 (D.C. Cir. 1984) (holding under the First Amendment, an FBI field investigation into an individual's political beliefs and associations must be subjected to an exacting standard).

37. *See, e.g.*, McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 347 (1995) ("When a law burdens core political speech, we apply 'exacting scrutiny,' and we uphold the restriction only if it is narrowly tailored to serve an overriding interest." (citation omitted)); *see also In re* Primus, 436 U.S. 412, 432 (1978) (stating that government-imposed burdens upon constitutionally protected communications must withstand exacting scrutiny and can be sustained only if the burdens are "closely drawn to avoid unnecessary abridgement of associational freedoms" (quoting Buckley v. Valeo, 424 U.S. 1, 25 (1976))).

38. *See* Tabbaa v. Chertoff, 509 F.3d 89, 92, 102 n.4 (2d Cir. 2007).

applying different legal standards . . . .[39]

In one especially important respect, the First Amendment affords expressive activities more protection from government surveillance than the Court's current Fourth Amendment jurisprudence. In a series of Fourth Amendment rulings dating back to 1974, the Court enforced the controversial third-party doctrine, holding that when a citizen voluntarily turns information over to a third party, those citizens have no Fourth Amendment right to challenge the government's efforts to get that information from those third parties.[40]

The Court's reasoning is that the Fourth Amendment only protects objectively reasonable expectations of privacy,[41] and that there is no such reasonable expectation concerning information that was already disclosed to third parties.[42] The government has invoked the third-party doctrine in defending its dragnet post-9/11 communications surveillance because there the government obtains the pertinent information from telephone service providers.[43] The third-party doctrine has been strongly criticized since the Court invented it, as being inconsistent with the Fourth Amendment.[44] Moreover, there are strong arguments that the cases in which the Court has enforced it are materially distinguishable from the dragnet communications surveillance now at issue.[45]

---

39. *Id.* at 102 n.4.

40. *See* Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 52 (1974); *see also, e.g.*, Smith v. Maryland, 442 U.S. 735, 742–46 (1979) (holding that phone users do not have a reasonable expectation of privacy in the "pen register" data maintained by third party phone companies); United States v. Miller, 425 U.S. 435, 437, 440, 444–45 (1976) (holding that bank records containing Miller's personal information were neither owned nor possessed by him and that the Fourth Amendment does not prohibit a third party from revealing that information).

41. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also* Missouri v. McNeely, 133 S. Ct. 1552, 1558–59 (2013) (affirming the reasonable expectation of privacy standard under the Fourth Amendment).

42. *Smith*, 442 U.S. at 743–44 (stating even if the Petitioner had a subjective expectation of privacy in the information voluntarily turned over to a third party, "this expectation is not 'one society was prepared to recognize as reasonable'" (quoting *Katz*, 389 U.S. at 361)).

43. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 33 (D.D.C. 2013).

44. *Smith*, 442 U.S. at 747–48 (1979) (Stewart, J., dissenting); *see also* Alexander Galicki, *The End of* Smith v. Maryland*?: The NSA's Bulk Telephony Metadata Program and the Fourth Amendment in the Cyber Age*, 52 AM. CRIM. L. REV. 375, 389–90 (2015).

45. *Klayman*, 957 F. Supp. 2d at 32 ("[T]he the Court in 1979 [could not] have ever imagined how the citizens of 2013 would interact with their phones. . . . [T]he

Even assuming arguendo that Fourth Amendment challenges to the bulk phone surveillance are rejected based on the third-party doctrine, the independent First Amendment claims would still survive. Although the Supreme Court has not addressed this issue, other courts have consistently held that litigants may assert First Amendment rights to the non-disclosure of information, regardless of who holds that information.[46] For example, the U.S. Court of Appeals for the Tenth Circuit held that bank customers may challenge the bank's disclosure of their customer records to the government on First Amendment grounds,[47] even though the Supreme Court had held that bank customers have no Fourth Amendment claim against such disclosure.[48] The bank customers in the Tenth Circuit case were two organizations, and as the court explained, their members' First Amendment "freedom to associate freely and anonymously . . . will be chilled equally whether the associational information is compelled from the organization itself or from third parties."[49] Likewise, a federal court struck down a mail cover under which the U.S. Postal Service recorded all information on the envelope or other outside cover of mail, on the grounds that it violated the First Amendment freedom of association, even though the court held that this mail cover did not violate the Fourth Amendment.[50] In a ruling directly pertinent to the current communications surveillance programs, the Second Circuit held that reporters could raise First Amendment challenges to the

---

surveillance program now before [the court] is so different from a simple pen register that *Smith* is of little value in assessing whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search.").

46. *See, e.g.*, *In re* Grand Jury Proceeding, 842 F.2d at 1229, 1233–34 (11th Cir. 1988) (rejecting the argument that the First Amendment affords no extra margin of privacy through additional restrictions on criminal investigations beyond those imposed by the Fourth and Fifth Amendments); Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n of N.Y. Harbor, 667 F. 2d 267, 271 (2d Cir. 1981) ("First Amendment rights are implicated whenever government seeks from third parties records of actions that play an integral part in facilitating an association's normal arrangements for obtaining members or contributions."); *see also* United States v. Citizens State Bank, 612 F.2d 1091, 1093 (8th Cir. 1980); Malibu Media v. Does, No. 12-2077, 2012 WL 3089383, at *6 (E.D. Pa. 2012); Rich v. City of Jacksonville, No. 3:09-cv-454-J-34MCR, 2010 WL 1141556, at *11 (M.D. Fla. 2010).

47. *In re* Grand Jury Subpoena First National Bank, Englewood, Colo., 701 F.2d 115, 118 (10th Cir. 1983).

48. United States v. Miller, 425 U.S. 435, 444–45 (1976).

49. In re *Grand Jury Subpoena First National Bank*, 701 F. 2d at 118.

50. Paton v. LaPrade, 469 F. Supp. 773, 781 (D.N.J. 1978). The court rejected the Fourth Amendment argument because the information at issue was visible to any number of postal workers. *Id.* at 777.

government's efforts to obtain their phone records from their phone companies.[51]

In some cases, compliance with Fourth Amendment requirements may also satisfy the First Amendment standards.[52] For example, a traditional search warrant, carefully drawn and supported by probable cause, may constitute the least restrictive means for pursuing important goals such as national security.[53] However, when the government sweeps up more information on a reduced showing of relevance or need, as is the case with the dragnet post-9/11 communications surveillance, the government is less likely to be able to meet its strict scrutiny burden.[54]

An important expert body known as the Privacy and Civil Liberties Oversight Board (PCLOB) made findings which support the First Amendment claims asserted by the plaintiffs in the ACLU and EFF lawsuits.[55] In its comprehensive 2014 report on the Section 215 bulk surveillance, the PCLOB concluded that the government's "bulk collection of telephone records [could] be expected to exert a substantial chilling effect on the activities of journalists, protestors, whistleblowers, political activists, and ordinary individuals."[56] It characterized this likely deterrence as rising

51. N.Y. Times Co. v. Gonzales, 459 F.3d 160, 163, 168 (2d Cir. 2006) ("[W]hatever rights a newspaper or reporter has to refuse disclosure in response to a subpoena extends to the newspaper's or reporter's telephone records in the possession of a third party provider.").

52. *See, e.g.*, Zurcher v. Stanford Daily, 436 U.S. 547, 565 (1978) ("[T]he prior cases do no more than insist that the courts apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search."); United States v. Ramsey, 431 U.S. 606, 623–24 (1977) ("First Amendment considerations dictate a full panoply of Fourth Amendment rights prior to the border search of mailed letters.").

53. *See Zurcher*, 436 U.S. at 565.

54. *See, e.g.*, Gibson v. Fla. Legislative Investigation Comm., 372 U.S. 539, 558 (1963) (declining to allow legislative inquiry into the broad topic of individual's associations on a lesser standard of relevance); FEC v. LaRouche, 817 F.2d 233, 234–35 (2d 1987) (holding the "FEC ha[d] failed to make . . . a showing with regard to the identities of the campaign's solicitors); Paton v. La Prade, 469 F. Supp. 773, 782 (D.N.J. 1978) (invalidating an FBI mail cover search on its face); *cf.* Local 1814 Int'l Longshoremen's Ass'n v. Waterfront Comm'n. of N.Y. Harbor, 667 F.2d 267, 269 (2d. Cir. 1981) (permitting disclosure of a limited number of individuals who authorized payroll deductions for contributions to an organization).

55. *See supra* notes 8–21 and accompanying text.

56. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND

to the level of a significant interference with the First Amendment right of political association, thus triggering exacting scrutiny.[57] In fact, it warned that this surveillance threatens to impose a unique chilling effect on speech and association because of the novel fact that "all calling records [of individuals and groups who desire privacy in their activities and associations] must be presumed to be in the hands of the government, under circumstances that give them no ability to know whether the government is scrutinizing their records or disseminating them to other agencies." [58] Moreover, the PCLOB concluded that this surveillance should fail exacting scrutiny because it is doubtful that it is sufficiently narrowly tailored to minimize this intrusion on associational rights.[59]

Worse yet, PCLOB and other experts concur that this dragnet surveillance does not make a significant contribution to advancing its anti-terrorism goals, which are effectively promoted by traditional targeted surveillance measures. [60] Therefore, the dragnet surveillance fails the necessary and least restrictive alternative aspects of strict scrutiny.[61] For example, the PCLOB's 2014 report, which reflected an in-depth examination of classified information, concluded:

> The Section 215 program has shown minimal value in safeguarding the nation from terrorism. Based on the information [the government] provided . . . including classified briefings and documentation, we have not identified a single instance . . . in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or

---

ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 135 (2014) [hereinafter PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT].

57. *Id.*

58. *Id.* at 167.

59. *Id.* at 135–36, 167–68.

60. *Id.* at 11, 146; *see also* LIBERTY AND SECURITY IN A CHANGING WORLD, REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 104 (2013) ("Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders.").

61. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT, *supra* note 56, at 167.

the disruption of a terrorist attack.[62]

A federal judge who ruled that this program violated the Fourth Amendment reached the same conclusion: "[T]he Government does *not* cite a single instance in which analysis of the NSA's bulk metadata collection actually . . . aided the Government in achieving any objective that was time sensitive in nature." [63] Likewise, a 2014 report by the New America Foundation, which analyzed all the terrorist plots that the government initially claimed had been thwarted in part due to the NSA's dragnet surveillance (before the evidence forced it to back away from these claims), concluded that such surveillance in fact had "no discernible impact on preventing acts of terrorism."[64]

The enormous adverse impact that Section 215 has on First Amendment rights is vividly demonstrated through the evidentiary submissions in the pending lawsuits,[65] as well as through amicus curiae briefs filed by a diverse range of organizations.[66] All attest to specific burdens that this surveillance imposes on their communications, with an adverse impact on their expressive and associational activities.[67] Additionally, the plaintiffs that are religious organizations document a chilling effect on their religious expression.[68]

For example, the most recent such lawsuit, which the ACLU filed in March 2015, *Wikimedia Foundation v. NSA*, was brought on behalf of the 500 million people who use Wikipedia every month, as well as a broad coalition of educational, human rights, legal, and media organizations whose work depends on the privacy of their communications.[69] The plaintiffs

62. *Id.* at 11.

63. Klayman v. Obama, 957 F. Supp. 2d 1, 40 (D.D.C. 2013).

64. Bailey Cahall et al., *Do NSA's Bulk Surveillance Programs Stop Terrorists?*, INTERNATIONAL SECURITY (Jan. 13, 2014), https://www.newamerica.org/international-security/do-nsas-bulk-surveillance-programs-stop-terrorists/.

65. *See, e.g.*, Plaintiff's Fed. Rule of Evidence Section 1006 Summary of Voluminous Evidence Filed in Support of Their Motion for Partial Summary Judgment and Opposition to the Gov. Defendant's Cross-Motion, Jewel v. NSA, No. 08-CV-4373-JSW (N.D. Cal. Nov. 09, 2012).

66. *See, e.g.*, Brief of Amicus Curiae First Amendment Orgs. in Support of Plaintiff's Opposition to Defendant's Motion to Dismiss at 2, Muslim Cmty Ass'n of Ann Arbor v. Ashcroft, No. 03-72913, 2003 WL 2385158 (E.D. Mich. Nov. 26, 2003).

67. *See, e.g., id.*

68. Complaint for Declaratory and Injunctive Relief at ¶ 41, Muslim Cmty. Ass'n of Ann Arbor v. Ashcroft, No. 03-72913, 2003 WL 23851817 (E.D. Mich. July 30, 2003).

69. Complaint for Declaratory Injunctive Relief at ¶ 2, Wikimedia Found. v. NSA,

include Amnesty International USA, [70] the National Association of Criminal Defense Lawyers,[71] and The Nation Magazine.[72] They challenge so-called "upstream surveillance" under the FAA.[73] The NSA conducts this surveillance by tapping directly into the Internet "backbone" inside the U.S.: "the network of high-capacity cables, switches and routers" across which Internet traffic travels.[74] The plaintiffs collectively engage in hundreds of billions of sensitive international communications over the Internet each year with "journalists, clients, experts, attorneys, civil society organizations, foreign government officials, and victims of human rights abuses, among others."[75] The upstream surveillance has a palpable chilling effect on all these communications, making it harder for the plaintiffs to gather information and share it with the general public.[76] For example, here is how officials of Wikimedia, the lead named plaintiff, explained the adverse chilling effect on the free exchange of knowledge and ideas that it, its users, and volunteers have experienced:

> [W]henever someone overseas views or edits a Wikipedia page, it's likely that the N.S.A. is tracking that activity . . . .
>
> . . . .
>
> During the 2011 Arab uprisings, Wikipedia users collaborated to create articles that helped educate the world about what was happening. Continuing cooperation between American and Egyptian intelligence services is well established . . . .
>
> So imagine, now, a Wikipedia user in Egypt who wants to edit a page about government opposition or discuss it with fellow editors. If that user knows the N.S.A. is routinely combing through her contributions to Wikipedia, and possibly sharing information with her government, she will surely be less likely to add her knowledge or have that conversation for fear of reprisal.

No. 1:15-CV-00662 (D. Md. Mar. 10, 2015).

70. *Id.* at ¶ 9.
71. *Id.* at ¶ 7.
72. *Id.* at ¶ 12.
73. *Id.* at ¶¶ 3, 40.
74. *Id.* at ¶ 40.
75. *Id.* at ¶¶ 2, 48.
76. *Id.* at ¶ 55.

> And then imagine this decision playing out in the minds of thousands of would-be contributors in other countries. That represents a loss for everyone who uses Wikipedia and the Internet[,] . . . hundreds of millions of readers in the United States and around the world.[77]

Similar chilling effects on expressive activities and associational rights were shown in a lawsuit that EFF began in the summer of 2013—promptly after the first Snowden revelations—challenging the NSA's bulk phone records surveillance under Patriot Act Section 215.[78] The plaintiffs in that lawsuit, *First Unitarian Church of Los Angeles v. NSA*, are 22 organizations including churches and other religions groups, a diverse range of membership and political advocacy organizations, and gun-ownership advocates.[79] Here is EFF's summary of how the government's mass communications surveillance has undermined these groups' First Amendment rights:

> [E]ach plaintiff has lost the ability to assure its members, supporters and constituents that . . . the telephonic communications between them will be kept confidential. . . . This ability to assure confidentiality is central to the plaintiffs' organizational missions. For example, many . . . who seek services from [the Council on American-Islamic Relations (CAIR)] . . . have been subject to government surveillance in the past. Discretion and confidentiality in communications are of paramount importance to them . . . .
>
> CAIR[] often works on international causes that . . . involve "countries of interest" to the U.S. government. . . . Because the government examines not only who persons of interest call, but also who those who receive those calls in turn call, CAIR[] has realized that when it calls people, it subjects them to increased government scrutiny. . . .
>
> Other plaintiffs have also experienced a decrease in telephone calls from their constituents. . . . Human Rights Watch knows that those who associate with and pass information to it are commonly subject to retaliation; it also believes that individuals have refrained from reporting human rights abuses to it because of concerns about the

77. Jimmy Wales & Lila Tretikov, *Stop Spying on Wikipedia Users*, N.Y. TIMES (Mar. 10, 2015), http://www.nytimes.com/2015/03/10/opinion/stop-spying-on-wikipedia-users.html?_r=0.

78. *See* Complaint for Constitutional Statutory Violations, Seeking Declaratory and Injunctive Relief, First Unitarian Church of L.A. v. NSA, No. 3:13-CV-03287 JSW 2013 WL 3678094, ¶ 70 (N.D. Cal. Jul. 16, 2013).

79. *Id.* at ¶¶ 16–33.

> security of such communications.
>
> Several other plaintiffs that operate telephone hotlines have similarly reported an abrupt drop in the number of calls that they receive .... For example,... Patient Privacy Rights Foundation (PPRF) saw its hotline calls halved .... PPRF believes that many of these lost callers were whistleblowers ....
>
> Many of the plaintiffs have heard from their constituents that they are highly concerned that the government now knows they have communicated with them. This concern has led these constituents to decrease their total engagement with plaintiffs, not just their telephone communications. [For example,] Media Alliance has had several of its members ask to terminate their memberships ....[80]

In *ACLU v. Clapper*, the ACLU challenges the mass communications surveillance on its own behalf and that of the NYCLU.[81] *Clapper* cites similar facts to substantiate the surveillance's adverse impact on their expressive activities:

> In the course of their work, Plaintiffs routinely communicate by phone with their members, donors, current and potential clients, whistleblowers, legislators and their staffs, other advocacy organizations, and members of the public. These communications are often sensitive or confidential; in many circumstances, that is true of the mere *fact* of the communication.
>
> The [surveillance] ... discourag[es] whistleblowers and others who would otherwise communicate with Plaintiffs ....[82]

Amicus curiae briefs filed in both lawsuits assert that the challenged bulk surveillance undermines First Amendment rights.[83] One such brief,

---

80. Plaintiff's Motion for Partial Summary Judgment That the Telephone Records Program is Unlawful Under Section 215 of the Patriot Act and the First Amendment, First Unitarian Church of L.A. v. NSA, No. 3:13-cv-03287 JSW, 2013 WL 6175512, at *20–22 (N.D. Cal. Nov. 6, 2013) (citations omitted).

81. ACLU v. Clapper, 785 F.3d 787, 799 (2d Cir. 2015).

82. Brief for Plaintiffs-Appellants, ACLU v. Clapper, (No. 14-42), 2014 WL 992414, at *53–54 (2d Cir. Mar. 7, 2014).

83. *See id.* at 54; Brief Amici Curiae for Reporters Committee for Freedom of the Press and 13 other organizations in support of Plaintiffs' Motion for Partial Summary Judgement at 4, First Unitarian Church of L.A. v. NSA, No. 3:13-cv-03287 JSW (N.D. Cal. Nov. 18, 2013) [hereinafter Brief for Reporters Committee for Freedom].

which was filed by 14 news organizations, explains how this surveillance has deterred whistleblowers and other confidential sources from providing valuable information, thus infringing on journalists' news gathering rights and undermining the public's right to information about what their government is doing in their name.[84] As the brief states:

> Confidentiality has been essential to the news media's constitutionally protected duty of providing information to the public about such matters as political corruption, national security and foreign affairs. Many history-altering news stories would not have been reported without confidential communications between journalists and sources.[85]

The brief quotes many journalists who note that their sources have dried up in the wake of revelations about the indiscriminate communications surveillance, even on subjects removed from national security.[86] For example, *New York Times* investigative reporter and three-time Pulitzer Prize winner David Barstow said, "I have absolutely no doubt whatsoever that stories have not gotten done because of this."[87]

Another noteworthy amicus brief was submitted in both the ACLU and EFF lawsuits by PEN American Center, a nonprofit writers' association that includes poets, playwrights, essayists, novelists, editors, screenwriters, journalists, literary agents, and translators.[88] This brief highlights the demonstrable deterrent effect that the mass surveillance has already had on writers, as shown in a survey that PEN commissioned in the fall of 2013.[89] The brief summarizes this chilling impact and states, "Writers are curtailing communications with sources and colleagues; they are avoiding writing about certain topics; and they are not pursuing research they otherwise would."[90] As the *New York Times* reported, the PEN survey shows that

---

84. Brief for Reporters Committee for Freedom, *supra* note 83, at 4.

85. *Id.*

86. *Id.* at 5–8.

87. *Id.* at 7 (quoting Jamie Schuman, *The Shadows of the Spooks*, REPORTERS COMM. FOR FREEDOM OF THE PRESS (2013), http://www.rcfp.org/browser-media-law-resources/news-media-law/news-media-and-law-fall-2013/shadows.spooks).

88. *See* Brief for PEN American Center, Inc. as Amicus Curiae Supporting Appellants, ACLU v. Clapper, (No. 14-42-cv), 2014 WL 1118038, at *1 (2d Cir. Mar. 13, 2014) [hereinafter Brief for PEN].

89. *Id.* at *21–24; PEN AMERICA, CHILLING EFFECTS: NSA SURVEILLANCE DRIVES U.S. WRITERS TO SELF-CENSOR 6–8 (2013).

90. Brief for PEN, *supra* note 88, at *2.

"more than a quarter" of the respondents "say[] that they have avoided, or are seriously considering avoiding, controversial topics in their work."[91]

The ACLU and Human Rights Watch (HRW) further documented the sweeping surveillance's negative impact on journalism in a detailed 2014 joint report.[92] The report was based in part on interviews with 46 journalists who cover intelligence, national security, and law enforcement for a wide range of news organizations, at least a dozen of whom have won Pulitzer Prizes and other prestigious awards.[93] The journalists explained that the mass surveillance intimidates sources, making them hesitate even to discuss unclassified matters of public concern.[94] The sources fear they could lose their security clearances, be fired, or even come under criminal investigation.[95] As one Pulitzer Prize winner commented, "People are increasingly scared to talk about anything."[96] This creates serious challenges for journalists who cover these important topic areas, because they are often working with information that is sensitive, even if it is not classified, and they need multiple sources to confirm the details of stories that may well be of great public interest.[97]

Many journalists described the elaborate techniques they had adopted to try to avoid creating evidence of their interaction with sources.[98] These techniques ranged from using encryption, disposable burner phones, air-gapped computers (which stay completely isolated from unsecured networks, including the Internet), and even abandoning electronic communications altogether.[99] Due to these cumbersome techniques, it is taking journalists much longer to gather information (when they can get it at all) so they are ultimately able to publish fewer stories.[100] As the ACLU

91. Noam Cohen, *Surveillance Leaves Writers Wary*, N.Y. TIMES (Nov. 11, 2013), http://www.nytimes.com/2013/11/12/books/pen-american-center-survey-finds-caution-among-members.html?smid=tw-share.

92. *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy*, HUMAN RTS. WATCH (July 28, 2014), https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and.

93. *See id.*

94. *Id.*

95. *Id.*

96. *Id.*

97. *Id.*

98. *Id.*

99. *Id.*

100. *See id.*

and HRW concluded, this situation curtails the public's ability to obtain important information about government activities and the media's ability to serve as a check on government.[101] Journalists also expressed concern that, rather than being treated as essential checks on government and partners in ensuring a healthy democratic debate, they are apparently "viewed as suspect for doing their jobs."[102] One prominent journalist summed up what many others also expressed: "I don't want the government to force me to act like a spy. I'm not a spy; I am a journalist."[103]

II. SECOND AMENDMENT

The government's bulk communications surveillance adversely impacts Second Amendment rights in a way that parallels its adverse impact on First Amendment rights. As gun-owners' rights groups have explained, individuals' reasonable fear that surveillance will disclose their purchase and use of firearms has deterred them from engaging in such activities, even though they are completely lawful and indeed protected by the Second Amendment.[104] The gun-owners' organizations recount past situations in which both government and private sector actors have misused identifying information about individuals who have lawfully exercised their Second Amendment rights, to subject them to various forms of harassment.[105] For example, they cite situations where government officials have confiscated lawfully acquired firearms, and where citizens have attempted to steal guns from and threatened the safety of lawful gun owners.[106] Recognizing this problem, Congress has passed multiple statutes that bar the creation of a national gun-registration system.[107] However, the ongoing bulk communications surveillance permits the government to amass the very same information, thus posing the very same threat to Second Amendment rights.[108] Indeed, the National Rifle Association's (NRA) amicus curiae brief in support of the ACLU's pending challenge to the mass Section 215

101. *Id.*
102. *Id.*
103. *Id.*
104. *See* Brief of Amicus Curiae Nat'l Rifle Ass'n of Am., Inc. In Support of Plaintiffs-Appellants, & Supporting Reversal at 15–17, ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015) (No. 14-42). The NRA has also asserted that the bulk phone surveillance deters it and its members from exercising First Amendment freedoms of speech and association. *See id.* at 5–12.
105. *Id.* at 16–17.
106. *Id.*
107. *Id.* at 19–20.
108. *Id.* at 22.

phone records surveillance explains that these phone records provide more accurate information about gun ownership than an official national registry would:

> Gathering and aggregating such private-sector records could allow the government to create a far more complete registry of actual or likely gun owners than could be created with government-mandated information .... For example, a person whose phone records show a pattern of repeated calls to gun stores, shooting ranges, and the NRA, is considerably more likely to be a gun owner than a person who makes no such calls.... The value of such information in identifying likely gun owners might dwarf the importance of an ATF [Bureau of Alcohol, Tobacco, Firearms and Explosives] record of a firearm purchased years ago from a now-defunct dealer, or a NICS [National Instant Criminal Background Check System] transaction record showing transfer of a firearm that may have been sold or given away as a gift.[109]

Notably, the PCLOB report stressed this NRA amicus brief in support of its conclusion that the bulk of Section 215 surveillance deters the exercise of additional constitutional rights,[110] beyond its conclusion that this surveillance may violate Fourth Amendment principles.[111]

Several gun-related organizations are co-plaintiffs in the Electronic Frontier Foundation's (EFF) *First Unitarian Church of Los Angeles* lawsuit, which is also challenging Section 215 surveillance: California Association of Federal Firearms Licensees; Calguns Foundation (CGF); and Franklin Armory.[112] For example, CGF is "a non-profit member-based organization" that "defends Californians who are unjustly accused of violating California's byzantine firearms laws while also working to vindicate the civil rights of California gun owners by challenging unconstitutional California laws."[113] CGF states that it runs an emergency hotline for gun owners in California who "are justifiably concerned about whether any of the firearms they own

---

109. *Id.* at 27–28.

110. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT, *supra* note 56, at 162.

111. *Id.* at 105.

112. Complaint for Constitutional and Statutory Violations, Seeking Declaratory and Injunctive Relief at ¶¶ 18–19, 21, First Unitarian Church of L.A. v. NSA, No. cv-13-3287-JSW (N.D. Cal. July 16, 2013).

113. Declaration of Gene Hoffman, Jr. for Calguns Found., Inc. in Support of Plaintiffs' Motion for Partial Summary Judgment at ¶ 2, First Unitarian Church of L.A. v. NSA, No. 3:13-cv-03287-JSW (N.D. Cal. Nov. 6, 2013).

are illegal in California as California makes the possession of ordinary firearms (in the other 49 states) a crime," and also "prohibit[s] certain combinations of cosmetic features on rifles or pistols."[114] CGF reports that since the Section 215 surveillance came to light, calls to its hotline, as well as other communications with it, have decreased because of the fear that the government could use such a communication to try to prove that the "law abiding gun owner knew she was committing a crime."[115] Similarly, Franklin Armory, which "designs, manufactures, and distributes firearms for resale . . . in the commercial marketplace," [116] has noted a 70 percent decrease in phone calls following the revelation of the Section 215 surveillance, with "customers articulat[ing] that they . . . [want to] avoid being targeted and identified as a gun owner."[117]

III. FIFTH AMENDMENT

Now, turning to the Fifth Amendment: The government's bulk communications surveillance program entails the massive seizure from private telephone companies of data they maintain about their customers, pursuant to orders issued by the (super) secret Foreign Intelligence Surveillance Court (FISC) in ex parte proceedings in which the government is the only party.[118] Moreover, the FISC's opinions are secret, even from the companies from which the data are seized.[119] To quote another one of Laura Donahue's Georgetown Law School colleagues, Professor Randy Barnett, "Secret judicial proceedings adjudicating the rights of private parties, without any ability to participate or even read the legal opinions of the judges, is the antithesis of the due process of law."[120] Likewise, in a lawsuit

---

114. *Id.* at ¶ 4.

115. *Id.* at ¶¶ 4, 6.

116. Declaration of Jay Jacobson for the Franklin Armory in Support of Plaintiffs' Motion for Partial Summary Judgment at ¶ 2, First Unitarian Church of L.A. v. NSA, No. 3:13-cv-03287-JSW(N.D. Cal. Nov. 6, 2013).

117. *Id.* at ¶ 4.

118. 50 U.S.C. § 1881b(c) (2012).

119. *See* ACLU v. FBI – *FISA Court Motions Requesting Public Access to Rulings on NSA Bulk Surveillance*, ACLU.ORG (Aug. 27, 2014), https://www.aclu.org/cases/aclu-v-fbi-fisa-court-motions-requesting-public-access-rulings-nsa-bulk-surveillance (noting that telecommunications company could not even disclose that the government demanded the records and that the subsequent opinions are treated as secret).

120. Randy E. Barnett, *The NSA's Surveillance is Unconstitutional*, WALL ST. J. (July 11, 2013), http://www.wsj.com/articles/SB10001424127887323823004578593591276402574.

brought by EFF, *First Unitarian Church of Los Angeles v. NSA*, the plaintiff argues that the government's interpretation of Section 215 as authorizing mass communications surveillance constitutes an unconstitutionally vague secret law, violating the Fifth Amendment Due Process Clause.[121] As EFF explains:

> Under the government's construction, the statute both lacks guidelines to prevent arbitrary and discriminatory surveillance and fails to apprise ordinary persons that it authorizes the government to acquire all of their phone records in bulk without any showing of suspicion or relevance. . . .
>
> Additionally, arbitrary and discretionary enforcement are especially problematic when, as here, the government's interpretation of a law is both secret and inconsistent with the law's plain language.[122]

In the *First Unitarian* lawsuit, EFF also challenges Section 215 bulk surveillance on two additional Fifth Amendment grounds: (1) that it violates the substantive due process right of informational privacy[123] and (2) that it violates the procedural due process right to notice and other protections required when the government infringes on informational privacy.[124]

The Supreme Court has recognized that the Fifth Amendment Due Process Clause substantively protects the individual interest in avoiding disclosure of personal matters.[125] Moreover, the Court has held that this

---

121. Complaint for Constitutional and Statutory Violations, Seeking Declaratory and Injunctive Relief at ¶ 86, First Unitarian Church of L.A. v. NSA, No. 3:13-cv-03287-JSW (N.D. Cal. Jul. 16, 2013).

122. Plaintiffs' Reply in Support of Plaintiffs' Motion for Partial Summary Judgment and Opposition to Defendants' Motion to Dismiss at 43, First Unitarian Church of L.A. v. NSA, No. 3:13-cv-03287-JSW (N.D. Cal. Apr. 25, 2014). For more discussion regarding the Supreme Court's analysis of statutory construction, see the cases compiled, *id.*, City of Chicago v. Morales, 527 U.S. 41, 60 (1999) (gang loitering statute facially unconstitutional because it lacked guidelines to prevent arbitrary and discriminatory enforcement and conferred "vast discretion" on the police); Kolender v. Lawson, 461 U.S. 352, 358 (1983) (statute criminalizing failure to provide "credible and reliable identification" vague because its lack of standards "vest[ed] virtually complete discretion in the hands of the police") (quotation marks omitted); Coates v. Cincinnati, 402 U.S. 611, 614 (1971) (statute aimed at "annoying" conduct vague "in the sense that no standard of conduct is specified at all").

123. Complaint for Constitutional and Statutory Violations, Seeking Declaratory and Injunctive Relief at ¶ 79, First Unitarian Church of L.A. v. NSA, No. 3:13-cv-03287-JSW (N.D. Cal. Jul. 16, 2013).

124. *Id.* at ¶ 81.

125. Whalen v. Roe, 429 U.S. 589, 599 (1977) (noting two different kinds of interests

Fifth Amendment right protects personal information even if it is known to third persons.[126] Accordingly, even if the third-party doctrine barred a Fourth Amendment challenge to the Section 215 bulk collection program, it should not bar the Fifth Amendment challenge. A government measure that infringes on informational privacy is subject to the heightened scrutiny that the Court applies to any measure infringing on a substantive due process right.[127] Therefore, PCLOB's conclusion, cited above in the First Amendment context, is relevant in this Fifth Amendment context too: the bulk surveillance is not sufficiently narrowly tailored to pass heightened scrutiny.[128] To the contrary, experts concur that the surveillance is not even effective in advancing its anti-terrorism goals, let alone necessary or the least restrictive alternative.[129] For this reason, it would even fail a less rigorous level of scrutiny.

Procedural due process requires the government to provide some notice and process before depriving a person of a liberty interest.[130] Specifically, the Supreme Court has enforced this essential procedural due process right in the post-9/11 context even on behalf of accused enemy combatants.[131] *A fortiori*, the right must be respected on behalf of all the

---

involved in protecting privacy, "[o]ne [being] the individual interest in avoiding disclosure of personal matters"); *see also* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 458–59 (1977) (recognizing a legitimate expectation of privacy "in matters of personal life"); Nelson v. NASA, 530 F.3d 865, 877 (9th Cir. 2008) ("We have repeatedly acknowledged that the Constitution protects an 'individual interest in avoiding disclosure of personal matters.'" (quoting *In re* Crawford, 194 F.3d 954, 958 (9th Cir. 1999))), *rev'd on other grounds*, 131 S. Ct. 746, 751 (2011) ("We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*").

126. *Nixon*, 433 U.S. at 458; *Nelson*, 530 F.3d at 880 n.5 ("The highly personal information that the government seeks . . . is protected by the right to privacy, whether it is obtained from third parties or from the applicant directly.").

127. *See In re* Crawford, 194 F.3d 954, 959 (9th Cir. 1999) (requiring government to show "its use of the information would advance a legitimate state interest and that its actions are narrowly tailored to meet the legitimate interest" (quoting Doe v. Attorney Gen., 941 F.2d 780, 796 (9th Cir. 1991))).

128. *See supra* notes 36–37 and accompanying text.

129. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT, *supra* note 56, at 11, 135, 146.

130. *See, e.g.*, Mathews v. Eldridge, 424 U.S. 319, 333, 349 (1976) (holding Due Process requires sufficient process regarding termination of social security disability payments).

131. Hamdi v. Rumsfeld, 542 U.S. 507, 535 (2004) (plurality opinion) (holding the basic due process requirements of notice and opportunity to be heard apply to

unsuspecting Americans whose informational privacy rights are being invaded under Section 215. Moreover, procedural due process rights are triggered by the government's deprivation of a liberty interest that is protected by statute, as well as one that is protected by the Constitution.[132] Therefore, even apart from the Fifth Amendment substantive due process right of informational privacy, federal statutes that protect phone-record privacy independently trigger procedural due process protections.[133] Yet, the government has provided no notice or process at all, not even after invading individuals' informational privacy rights, let alone before.

IV. SIXTH AMENDMENT

Now, consider the Sixth Amendment right of the accused "[i]n all criminal prosecutions, . . . to have the Assistance of Counsel for his defence."[134] An amicus brief submitted by the National Association of Criminal Defense Lawyers (NACDL) raises this issue in a lawsuit brought by the EFF, *First Unitarian Church of Los Angeles v. National Security Agency*.[135] It explains that the bulk phone surveillance vitiates the confidentiality of attorney-client communications, thereby chilling them.[136]

Citing professional responsibility standards and court rulings,[137] the NACDL explains that defense counsel "have a unique obligation to ensure the confidentiality of their communications with, and on behalf of, their clients, . . . and to avoid employing means of communication that may compromise that confidentiality."[138] However, due to the bulk phone surveillance, using any electronic communication now compromises confidentiality—absent the burdensome, expensive methods that journalists must also use for confidentiality reasons as discussed earlier.[139] As the NACDL concluded in their brief in support of Plaintiffs' Motion for Summary Judgment in the *First Unitarian* case, "In a world where every

---

individuals challenging governmental determinations of enemy combatant status).

132. *See Eldridge*, 424 U.S. at 333, 349 (stating due process applies to social security disability benefits).

133. *See, e.g.*, 18 U.S.C. §§ 2702(a)(1)–(3), 2703(d) (2012).

134. U.S. CONST. amend. VI.

135. *See* Brief of the National Ass'n of Criminal Defense Lawyers as Amicus Curiae in Support of Appellant at 4–5, Smith v. Obama, No. 14-35555 (9th Cir. Sept. 9, 2014).

136. *Id.* at 9, 12.

137. *Id.* at 6.

138. *Id.* at 8.

139. *See supra* notes 92–103 and accompanying text.

reasonable modern method of communication is apparently subject to routine mass seizure by the Government, the right to consult with counsel, under the protection of the attorney-client privilege, simply disappears."[140]

V. ARTICLE III

The final constitutional problem with ongoing mass communications surveillance specifically applies to surveillance conducted under Section 702 of the 2008 FISA Amendments Act (FAA). The role that the FISC plays under the FAA requires it to issue abstract advisory opinions in violation of Article III of the Constitution.[141] The FAA requires the FISC to review the legality and constitutionality of the government's programmatic procedures in the abstract, with no concrete factual context concerning particular surveillance targets.[142]

The Brennan Center recently issued a report on the FISC, which critiqued the FAA surveillance under Article III,[143] and further noted that there are similar problems with the Section 215 bulk surveillance.[144] As it explained: "This program, too, now involves judicial approval, without any adversarial process, of the broad contours of a program affecting much of the American population—a situation that cannot be squared with . . . Article III."[145] The ACLU raised the Article III problem in its challenges to FAA surveillance in the *Wikimedia v. NSA* lawsuit.[146]

The Article III problems with the FAA can be highlighted by

---

140. Brief of the National Ass'n of Criminal Defense Lawyers as Amicus Curiae Supporting Plaintiffs' at 6, First Unitarian Church of L.A. v. NSA, No. 3:13-cv-03287 JSW (N.D. Cal. Nov. 18, 2013).

141. ELIZABETH GOITEN & FAIZA PATEL, BRENNAN CTR. FOR JUST., WHAT WENT WRONG WITH THE FISA COURT 7 (2015) [hereinafter WHAT WENT WRONG]; *see also* Flast v. Cohen, 392 U.S. 83, 96 (1968) ("[T]he implicit policies embodied in Article III, and not history alone, impose the rule against advisory opinions on federal courts."). Article III requires that federal courts rule only on concrete cases and controversies. U.S. CONST. art. III, § 2.

142. *See* WHAT WENT WRONG, *supra* note 141, at 27 ("Under Section 702, . . . the court has no role in approving individual intrusions at all. Rather, its substantive role is limited to determining whether generic sets of targeting and minimization procedures comply with the statute . . . and with the Fourth Amendment.").

143. *Id.* at 4, 7.

144. *See id.* at 29–33.

145. *Id.* at 30.

146. Complaint for Declaratory and Injunctive Relief at ¶ 1, Wikimedia Found. v. NSA, No. 1:15-CV-00662-RDB (D. Md. Mar. 10, 2015).

contrasting the FISC's role under the FAA with its completely different role under the original 1978 Foreign Intelligence Surveillance Act (FISA). FISA incorporated standards quite close to the Fourth Amendment requirements of a judge-issued warrant based "upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized."[147] FISA surveillance was confined to specific targets and specific facilities or places; it required a specific FISC warrant; this warrant in turn could only be based on the FISC's finding that (a) the specific target was a foreign power or agent of a foreign power, and (b) that each of the specifically identified facilities or places at which the surveillance was directed was being used, or about to be used, by a foreign power or an agent of a foreign power.[148]

In contrast, under the FAA, the government may conduct dragnet surveillance of all international communications entering or leaving the U.S., including those sent or received by U.S. citizens.[149] Completely contrary to its role under FISA, under the FAA the FISC does not approve surveillance of any specific target, facilities, or places.[150] Instead, the FISC approves only the general procedures that the government uses to carry out its mass surveillance, and it does this by issuing an aptly labeled mass-acquisition order.[151] This order is based upon the government's submission, for the FISC approval, of so-called targeting procedures and minimization procedures.[152] These procedures must be reasonably designed to ensure that the acquisition targets persons "reasonably believed to be located outside the United States" and also to minimize the acquisition and retention of information about U.S. citizens.[153] In sum, under the FAA, FISC broadly approves vague parameters under which the government is free to conduct dragnet surveillance for up to one year.[154]

Since the earliest days of our Republic, the Supreme Court has held

147. *Compare* U.S. CONST. amend. IV, *with* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 105, 92 Stat. 1783, 1790 (1978) (codified as amended at 50 U.S.C. § 1804 (2012)).

148. *See* Foreign Intelligence Surveillance Act § 104, 92 Stat. at 1788–90.

149. *See* Foreign Intelligence Surveillance Amendment Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2438 (codified in 50 U.S.C. § 1881a (2012)).

150. *See id.*

151. *Id.*

152. *Id.* § 702(c)(1)(A), 122 Stat. at 2938.

153. *Id.* § 702(d)(1)(A)–(B), 122 Stat. at 2439.

154. *See id.* § 702(a), 122 Stat. at 2438.

that federal courts are barred from issuing advisory opinions.[155] Advisory opinions are abstract declarations of the law, untethered to a specific, concrete dispute between particular adverse parties.[156] The purpose of this fundamental limitation, consistent with our Constitution's overall system of divided and checked powers, is to bar federal judges from policymaking, which instead is the province of electorally-accountable officials. [157] Accordingly, federal judges may not make abstract pronouncements about broad legal principles, but rather must only "appl[y] principles of law or equity to facts" that are presented by specific parties who seek the adjudication of a particular controversy.[158]

Under the FAA, the FISC's role is precisely the opposite of what Article III requires. It is not restricted to adjudicate any specific controversy about any particular surveillance target, but instead it is empowered to opine on general rules that govern a broad surveillance program.[159] That function is traditionally and appropriately performed not by an Article III federal court, but rather by an administrative agency.[160] In fact, former FISC judge James Robertson made precisely this charge: "The [FAA] has turned the FISA court into an administrative agency making rules for others to follow."[161] He expressly noted the reason why a federal court may not serve in this role: "It is not the bailiwick of judges to make policy."[162]

The conclusion that the FISC's rulings under the FAA constitute impermissible advisory opinions is reinforced by the reasons that federal courts and the Justice Department stressed in reaching the opposite conclusion about the FISC's rulings under the original 1978 FISA. These reasons consisted of qualities that distinguish FISC's role under FISA from its role under the FAA. Specifically, in holding that FISA did not empower

155. *See* Flast v. Cohen, 392 U.S. 83, 96 (1968) (stating the rule against advisory opinions in federal courts is well-settled); 13 CHARLES ALAN WRIGHT, ARTHUR R. MILLER & EDWARD H. COOPER, FEDERAL PRACTICE & PROCEDURE § 3529.1 (2008) ("The oldest and most consistent thread in the federal law of justiciability is that the federal courts will not give advisory opinions." (citations omitted)).

156. *See, e.g.*, *In re* Summers, 325 U.S. 561, 566–67 (1945).

157. *See* United States v. Smith, 686 F. Supp. 847, 855 (D. Colo. 1988).

158. Vermont v. New York, 417 U.S. 270, 277 (1974).

159. See § 702(a), 122 Stat. at 2438.

160. *See* AM. JUR. 2D *Administrative Law* §§ 45, 67 (2015).

161. Dan Roberts, *U.S. Must Fix Secret FISA Courts, Says Top Judge who Granted Surveillance Orders*, THE GUARDIAN (July 10, 2013), http://www.theguardian.com/law/2013/jul/09/fisa-courts-judge-nsa-surveillance (quotation marks omitted).

162. *Id.* (quotation marks omitted).

the FISC to issue advisory opinions, courts stressed that FISA cases "involve concrete questions respecting the application of the Act" to particular proposed surveillance targets.[163] For example, one court said that a FISC judge who is asked to rule on a traditional FISA warrant application, "is not faced with an abstract issue of law or called upon to issue an advisory opinion, but is, instead, called upon to ensure that the individuals who are targeted do not have their privacy interests invaded, except in compliance with the detailed requirements of the statute."[164] Likewise, when the original FISA was being debated, the Justice Department's Office of Legal Counsel emphasized that the FISC complied with Article III because it would "apply standards of law to the facts of a particular case."[165] In sum, the very reasons why the judicial and executive branches concurred that FISC's role under the original FISA did not violate Article III underscore that FISC's diametrically different role under the FAA is incompatible with Article III.

The Article III problems with FISC's role under the FAA are compounded by the fact that the government may disregard any FISC ruling denying its application for a mass acquisition order pending appeal.[166] Both Article III and separation of powers principles mandate that judicial decisions must be binding on the parties unless they are stayed, modified, or reversed within the judicial process itself.[167] In contrast, unenforceable rulings, which another branch of government may ignore at will, are not in fact judicial decisions consistent with Article III, but rather impermissible advisory opinions.[168] FAA orders disapproving acquisitions are denied the

---

163. *See, e.g.*, United States v. Megahey, 553 F. Supp. 1180, 1197 (E.D.N.Y. 1982), *aff'd sub nom.* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

164. *Id.*

165. Memorandum from John M. Harmon, Assistant Att'y Gen., OLC, to Hon. Edward P. Boland, Chairman, House Permanent Select Comm. On Intelligence (Apr. 18, 1978), *reprinted in Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legis. of the H. Permanent Select Comm. On Intelligence*, 95th Cong. 28 (1978).

166. 50 U.S.C. § 1881a(i)(4)(B)(i)–(ii).

167. *See* Plaut v. Spendthrift Farm, Inc., 514 U.S. 211, 218–19 (1995) (holding that the judicial power is to render dispositive judgments, which decide cases, subject to review only by superior courts in the Article III hierarchy); Chicago & S. Air Lines, Inc. v. Waterman S.S. Corp., 333 U.S. 103, 113 (1948) ("Judgments . . . may not lawfully be revised, overturned or refused faith and credit by another Department of Government.").

168. *See generally* 1 LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW § 3–9 (3d ed. 2000) (explaining that Article III courts will not issue advisory opinions

dispositive character that is the essential element of the federal judicial power.[169] By providing for judicial review of general procedures that the executive branch draws up but excusing the executive from any duty of prompt compliance, the FAA violates Article III.[170]

In conclusion, the ongoing dragnet communications surveillance programs raise multiple statutory and constitutional problems. Each problem alone, and even more so the whole combination, provides a serious ground at least for vastly curbing such programs, if not ending them.

concerning legislative or executive action).

169. *See Chicago & S. Air Lines, Inc.*, 333 U.S. at 113 (noting decisions of Article III courts which are made within the powers of those courts are binding).

170. In addition, by denying the judiciary the power to demand compliance with its orders, the FAA in effect imposes a rule of decision on the courts, mandating a de facto stay violating the holding in *United States v. Klein*. *See* 80 U.S. 128, 147 (1871) ("It is the intention of the Constitution that each of the great co-ordinate departments of the government—the Legislative, the Executive, and the Judicial—shall be, in its sphere, independent of the others.").