THE SYNERGY OF PRIVACY AND SPEECH

Nicole B. Cásarez[*]

TABLE OF CONTENTS

---

* Visiting Professor of Law, University of Houston Law Center; Professor, Communication, University of St. Thomas, Houston, Texas. University of Texas, B.J., 1976, J.D. 1979; University of Houston, M.A. 1991. I would like to thank Peter Linzer and Emily Berman, both of the University of Houston Law Center, for their encouragement and their helpful comments on earlier drafts. Any errors that remain are mine alone.

INTRODUCTION

However history ultimately judges Edward Snowden, his 2013 revelations regarding secret bulk collection of domestic phone records by the National Security Agency ("NSA") eroded many Americans' trust in their government, as well as their confidence in the privacy of their electronic conversations.[1] Americans were shocked and angered to learn that their government had been collecting all kinds of information about their communications, without serious judicial supervision and when most or all of the data was domestic. Fears that America had turned into a surveillance state fueled sales of encryption technology[2] and were reflected in both the media and popular culture.[3]

1 *See, e.g.*, Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, 23–25 (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf [hereinafter Pew 2014 Study] (finding that, with respect to landline phones, cell phones, text messaging, instant messaging, email, and social media messaging, "there is not one mode through which a majority of the American public feels 'very secure' sharing private information with another trusted person or organization").

2 *See e.g.*, Bill Flook, *There's No Business Like Snowden Business*, WASH. BUS. J. (July 25, 2014), http://www.bizjournals.com/washington/print-edition/2014/07/25/theres-no-business-like-snowden-business.html?page=all (describing how consumer interest in encryption technology increased following the Snowden disclosures).

3 Journalists covering the Snowden revelations inevitably invoked George Orwell. *See* PEN Surveillance Mapping Metaphor Project, PEN American Ctr., http://www.pen.org/infographic/pen-surveillance-metaphor-mapping-project (illustrating that Orwell's novel *1984* was the only literary work referred to in the PEN America survey).

Government surveillance also inspired art exhibits, songs, and even a popular Hollywood children's movie. *See, e.g.*, Peter Maass, *Art in a Time of Surveillance*, First Look, THE INTERCEPT, Nov. 13, 2014, https://firstlook.org/theintercept/2014/11/13/art-surveillance-explored-artists; John Hanlon, *Why* The LEGO Movie *is the new* Nineteen Eighty-Four, THE WEEK, Feb. 7, 2014, http://theweek.com/article/index/256154/why-the-lego-movie-is-the-new-nineteen-eighty-four (comparing the influence of government surveillance in Orwell's *1984* and *The LEGO Movie*); Rock, Paper, Cynic, *Hello NSA (A Love Song of Mass Surveillance)*, YOUTUBE (Feb. 11, 2014), https://www.youtube.com/watch?v=Eiu-7Ij6CWI.

After two years of public debate and political grandstanding, Congress finally enacted the USA FREEDOM Act,[4] and news reports trumpeted the end of government bulk collection of American telephone records.[5] No longer could the government use Section 215 of the USA PATRIOT Act[6] to force telecommunications providers to deliver to the NSA, on a daily basis, the "metadata"—transmittal information including the numbers dialed, time, date, and duration[7]—associated with most Americans' phone calls.[8] Both President Barack Obama and Edward Snowden applauded the passage of the new law,[9] the latter calling it "a historic victory for the rights of every citizen."[10]

---

4 Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection, and Online Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268, codified at 50 U.S.C. § 1861 (2015) [hereinafter Freedom Act].

5 *See, e.g.*, David Cole, *Reining in the NSA*, N.Y. TIMES REV. OF BOOKS (June 2, 2015), http://www.nybooks.com/blogs/nyrblog/2015/jun/02/nsa-surveillance-congress-sunset; Sabrina Siddiqui, *Congress Passes NSA Surveillance Reform in Vindication for Snowden*, THE GUARDIAN (June 3, 2015), http://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden.

6 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56, 115 Stat. 272 (codified in scattered titles of the U.S.C.) [hereinafter Patriot Act]. Section 215 of the Patriot Act amended the "business records" provision of the Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 8, 18 and 50 U.S.C.) [hereinafter FISA]. The business records provision authorizes the FBI Director or a designee to seek:

> an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

Patriot Act, codified as amended at 50 U.S.C. § 1861(a). The application for such authority need only "specify that the records concerned are sought for an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." *Id.*, codified as amended at 50 U.S.C. § 1861(b)(2).

7 *See* David Medine et al., *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*, Privacy & Civil Liberties Oversight Bd. 8 (2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf [hereinafter PCLOB Section 215 Report] (defining "metadata" for phone calls and emails).

8 To be more precise, the Freedom Act authorized the government to restart the former Section 215 program and operate it for six months while the NSA and the telecommunications providers transition to the new, Freedom Act system. Freedom Act, *supra* note 4, at § 109(a).

9 *See* Jennifer Steinhauer & Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 is Sharply Limited*, N.Y. TIMES, June 3, 2015, at A1 (noting that "Mr. Obama was quick to praise passage of the legislation and to scold those who opposed it").

10 Edward J. Snowden, *Edward Snowden: The World Says No to Surveillance*, N.Y. TIMES, June 5, 2015, at A27.

Politicians and professors labeled the Freedom Act the most significant surveillance reform in decades, describing it as a reflection of the popular belief that the government has no business spying on Americans' calls.[11] Some went so far as to give credit to Snowden for launching a debate that led to legislative reform, resulting in a paradigmatic example of the democratic process at work.[12]

In fact, however, these laudatory remarks overstate what the Freedom Act actually accomplished. While the new law imposes some limits on the government's ability to gather Americans' domestic communications records under the Patriot Act, the Freedom Act leaves untouched the government's power to collect most (if not all) of these same records under other legal authorities. These other laws include Executive Order ("EO 12333"),[13] issued by President Ronald Reagan in 1981, which sets out an expansive framework under which the nation's intelligence agencies engage in surveillance activities conducted outside U.S. borders without judicial involvement or meaningful congressional oversight.[14] Although Title VII of the For-

11 *See, e.g.*, Erin Kelly, *Senate Approves USA Freedom Act*, USA TODAY (June 2, 2015), http://www.usatoday.com/story/news/politics/2015/06/02/patriot-act-usa-freedom-act-senate-vote/28345747 ("Americans are no longer willing to give the intelligence agencies a blank check."); Peter Swire, *The USA FREEDOM Act, the President's Review Group and the Biggest Intelligence Reform in 40 Years*, PRIVACY PERSPECTIVES (June 8, 2015), https://privacyassociation.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years/ (calling the USA FREEDOM Act the "biggest pro-privacy change to U.S. intelligence law since the original enactment of the Foreign Intelligence Surveillance Act in 1978").

12 *See, e.g.*, Cole, *supra* note 5; Jessica Shulberg, *The Elephant in the Room: Senators Finally Credit Snowden For Role in Patriot Act Reforms*, HUFFINGTON POST (June 1, 2015), http://www.huffingtonpost.com/2015/06/01/snowden-nsa-patriot-act_n_7485702.html.

13 Exec. Order No. 12333, 3 C.F.R. 200 (1981), amended by Exec. Order No. 13284, 3 C.F.R. 161 (2003); Exec. Order No. 13355, 3 C.F.R. 218 (2004); and Exec. Order No. 13470, 3 C.F.R. 218 (2008) [hereinafter EO 12333]. EO 12333 explains that, under its auspices, "[a]ll means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used to obtain reliable intelligence information to protect the United States and its interests." *Id.* §1.1(a). Its provisions are implemented by individual intelligence agencies pursuant to guidelines that must be approved by the Attorney General. *Id.* § 3.2.

The full text of EO 12333, as amended, is available online. *See, e.g.*, EO 12333, http://fas.org/irp/offdocs/eo/eo-12333-2008.pdf.

14 *See* Nat'l Sec. Agency, Memorandum: The National Security Agency: Missions, Authorities, Oversight and Partnerships, 2 (Aug. 9, 2013), https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf [hereinafter NSA Memorandum] (stating that EO 12333 applies when surveillance is "conducted through various means around the globe, largely from outside the United States, which is not otherwise regulated by FISA").

eign Intelligence Surveillance Act of 1978 ("FISA")[15] forbids the government from intentionally targeting a U.S. person's foreign communications without a FISA warrant,[16] bulk collection of communications from abroad is regarded by the NSA as not targeting anyone.[17] These large-scale collections under EO 12333 cannot avoid "incidentally" harvesting sizeable quantities of U.S. person communications, including, for example, both content and metadata of calls made by Americans to or from a foreign country, or even purely domestic communications that travel over international cables or are stored on backup servers located in foreign countries.[18] For this reason, EO 12333 has been described as a legal loophole by which the NSA can avoid complying with FISA or the Fourth Amendment even as the agency intercepts communications belonging to Americans.[19] Although by passing the Freedom Act, Congress has showed itself willing to make changes to the surveillance state, the surveillers have yet to be reined in.

All government surveillance programs create communications privacy concerns, whether the snooping consists of a government agent opening a sealed letter, wiretapping a telephone, pretending to be a criminal suspect's trusted friend, or collecting and analyzing communications metadata. When we communicate with others, both the right to privacy and the right of free expression are put in play. Communications privacy promotes both individual and societal values; it enables us to engage in meaningful social interactions that are essential to both the creation of intimate personal relationships and the maintenance of a flourishing political system. Logically, then, it would follow that in America we ought to accord significant constitutional protection, based on both the Fourth and First Amendments, to the privacy of our communications.

Generally, however, questions regarding the ability of speakers to exclude the "uninvited ear"[20] of the government from our communications have been treated by courts as governed entirely by the Fourth Amendment, not the First. If the surveillance in question qualifies as a search or seizure under the Fourth Amendment, any First Amendment implications are adequately addressed, according

15 Title VII was added to the original FISA in the FISA Amendments Act of 2008, Pub. L. 110-161, 122 Stat. 2436 (July 10, 2008).

16 FISA, *supra* note 6, at § 1881c(a)(2).

17 *See infra* notes 77–79 and accompanying text.

18 *See infra* notes 80–81 and accompanying text.

19 *See infra* notes 82–88 and accompanying text.

20 Katz v. United States, 389 U.S. 347, 352 (1967).

to the Court, if the government obtains a warrant.[21] If the surveillance does not rise to the level of a search or seizure because the government collects only non-content communications metadata that the speaker shared with a third party, not even a warrant is required.[22]

Nevertheless, scholars have repeatedly called for recognition of a First Amendment right to be free from government surveillance, whether because it interferes with the freedom of thought necessary for what Professor Neil Richards has termed "intellectual privacy,"[23] or, because as Professor Katherine Strandburg has argued, surveillance that reveals citizens' organizational ties violates freedom of association.[24] So far, these arguments have failed to gain much traction. Declassified Foreign Intelligence Surveillance Court ("FISC" or "FISA court") opinions that authorized bulk collection of communications metadata under FISA either rejected any First Amendment objections or failed to mention them at all.[25] While several lawsuits challenging surveillance programs have raised First Amendment claims, those arguments either did not prevail or were not addressed by courts.[26]

My central theme is that the First Amendment should be considered in partnership with the Fourth so that both play a role in determining the constitutionality of bulk government surveillance of our communications. Given the development of the law and the constraints of precedent, neither Amendment will, on its own, provide

---

21 *See infra* notes 324–29 and accompanying text.

22 *See infra* notes 141–49, 181–86 and accompanying text.

23 *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013).

24 *See* Katherine J. Strandburg, *Membership Lists, Metadata, and Freedom of Association's Specificity Requirement*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 327, 332 (2014).

25 *See, e.g.*, Opinion and Order, [Redacted], No. PR/TT [Redacted] at 66-69 (FISA Ct. [Redacted] 2004) (Kollar-Kotelly, J.), https://www.documentcloud.org/documents/836336-cleanedprtt-1.html [hereinafter Kollar-Kotelly Opinion] (holding that NSA bulk collection of email and Internet metadata under Section 214 of the Patriot Act did not violate the First Amendment); Amended Memorandum Opinion, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], No. BR 13-109 (FISA Ct. Aug. 29, 2013) (Eagan, J.), http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf [hereinafter Eagan opinion] (upholding Section 215 program under the Fourth Amendment with no mention of the First Amendment).

26 *See, e.g.*, ACLU v. Clapper, 785 F.3d 787, 821 n.12 (2d Cir. 2015) (deciding the cases without reaching the First Amendment issue); United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 U.S. Dist. LEXIS 85452, at *30–38 (D. Ore. June 24, 2014) (holding that surveillance under Section 702 of FISA did not violate the First Amendment because the Fourth Amendment was satisfied); Klayman v. Obama, 957 F. Supp. 2d 1, 9–10 n.7 (D.D.C. 2013) (enjoining operation of Section 215 program on Fourth Amendment grounds, without reaching the First Amendment claim), *rev'd*, 800 F.3d 559 (D.C. Cir. 2015).

sufficient protection against the government with respect to communications privacy. My specific focus here is on government collection and analysis of communications metadata under EO 12333.[27] While the Freedom Act represents a small step by Congress to improve our communications privacy, it did nothing to resolve the great constitutional metadata debate. It leaves intact the government's overarching legal theory that when the NSA collects communications metadata and uses it to map out our contacts and social networks (what the NSA calls "contact chaining"[28]), the agency resides in a Constitution-free zone. [29]

In Part I, I give a brief overview of the Freedom Act, and contrast it with what we know about the government's ability incidentally to collect domestic communications pursuant to EO 12333. While the Freedom Act places some restraints on the NSA's ability to hold and analyze domestic metadata, most of the public remains unaware that EO 12333 provides an alternate authority for the NSA to engage in many of the same activities while bypassing any statutory or constitutional limitations.

In Part II, I describe how communications privacy developed under the Fourth rather than the First Amendment. I show how the Court's reasonable expectation of privacy test from the electronic eavesdropping cases, combined with the assumption of the risk concept developed in the false friend cases evolved into the notorious third party doctrine. This much-criticized legal principle forms the basis for the government's constitutional argument justifying bulk

---

27 This is not to discount the importance of the First and Fourth Amendments with respect to government collection of communication content. However, when the government collects communications content under FISA or, to a more limited extent, under EO 12333, certain minimization requirements apply that limit the acquisition, retention, and dissemination of non-publicly available U.S. person information. *See infra* notes 91–93 and accompanying text. Whether those protections adequately safeguard First and Fourth Amendment interests is a topic for another day; for present purposes, I note that minimization procedures regarding the analysis of communications metadata collected under EO 12333 are much less robust. *See infra* notes 94–109 and accompanying text.

For a comprehensive analysis of the statutory and constitutional issues regarding international collection of communications content under FISA, see generally Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117 (2015).

28 *See* PCLOB Section 215 Report, *supra* note 7, at 26–31 (explaining the contact chaining process in the context of the former Section 215 telephony metadata program).

29 *See* ADMIN. WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 19–22 (2013), https://info.publicintelligence.net/DoJ-NSABulkCollection.pdf [hereinafter ADMIN. WHITE PAPER] (defending former Section 215 telephony metadata program as constitutional under both the Fourth and First Amendments).

collection and analysis of domestic metadata in general, and under EO 12333 in particular.[30] Although commentators have made strong and thoughtful arguments as to why the third party doctrine should be jettisoned as a relic of a bygone era,[31] whether the Supreme Court is ready to do so remains uncertain.

Part III explains why stand-alone First Amendment challenges to bulk government collection of communications metadata are also unlikely to succeed. Government monitoring of our communications activity, including gathering and analyzing communications metadata, would logically seem to inhibit speech. However, chilling effects by themselves are not a sufficient injury to support a First Amendment claim, and government surveillance programs neither prohibit nor punish speech.[32] Associational privacy claims provide a somewhat stronger argument, but without evidence of retaliation or other negative effects, they are also likely to fail.[33] As a result, even massive surveillance programs that collect and analyze communications metadata belonging to U.S. persons, such as the little-known EO 12333, are unlikely to be struck down as violations of the First Amendment.

In Part IV, I describe how the Supreme Court has, nevertheless, recognized the salience of First Amendment values when the government interferes with our communications privacy. In particular, I focus on *United States v. U.S. District Court* (the "*Keith*" case),[34] where the Court indicated that when the government captures communications content in national security cases, the First Amendment should be read in conjunction with the Fourth Amendment to provide parties to those communications with heightened privacy protections.[35] This, I believe, will provide a path for the Court to reevaluate and limit the third party doctrine with respect to dragnet government collection of communications metadata without overruling the doctrine entirely. By determining that communications metadata associated with U.S. person communications that the NSA happens to capture abroad—whether because an American called a person in a foreign country, or because a wholly domestic communication traveled through a transoceanic cable—are relevant to foreign intelligence investigations such that they can be captured and contact-chained without limit, the government has engaged in an end-run around

30 *See infra* notes 181–88 and accompanying text.
31 *See infra* notes 153–54 and accompanying text.
32 *See infra* notes 241–61 and accompanying text.
33 *See infra* notes 262–79 and accompanying text.
34 407 U.S. 297 (1972).
35 *Id.* at 313–14.

Keith's holding that it must procure a warrant to engage in electronic surveillance of U.S. citizens with "no significant connection with a foreign power, its agents or agencies."[36]

Whether a constitutional challenge to bulk incidental collection of domestic metadata under EO 12333 will ever be heard by the Supreme Court is another matter. Standing doctrine as currently applied by the Court has prohibited constitutional review of surveillance programs where the plaintiffs cannot demonstrate that their communications were, in fact, gathered or scrutinized by the government.[37] Many have argued that in the context of massive government surveillance programs, the Court should loosen standing requirements and recognize a broader range of harms to ensure that those programs do not escape judicial review.[38] Given the serious implications that unchecked executive branch surveillance power presents to privacy, speech, and our democratic process, this would be a welcome development. Courts must abandon overly narrow views of standing that make it impossible to challenge clear violations of law.

In the meantime, however, I conclude by calling for both Congress and the executive branch to act to bring the NSA's incidental collection of domestic communications metadata under EO 12333 more in line with the Fourth and First Amendments. As a start, both Congress and the public need as much information as national security permits regarding the scope and efficacy of those collection efforts. Additionally, I sketch out further congressional and executive branch reforms that would provide meaningful privacy protections to American communication records that the government currently can harvest from abroad. If enacted, these reforms would help create a world in which we need not fear that the government collects, analyzes, and stores the records of our everyday communications simply because, thanks to technology, those records can be obtained from foreign sources.

---

36 *Id.* at 309 n.8.

37 Clapper v. Amnesty Int'l USA,133 S. Ct. 1138, 1148 (2013). *See infra* notes 280–307 and accompanying text.

38 *See, e.g.*, Richards, *supra* note 23, at 1963 (proposing that the Supreme Court should recognize surveillance of intellectual activities as a harm in standing doctrine); Christopher Slobogin, *Standing and Covert Surveillance*, 42 PEPP. L. REV. 517, 519–20 (2015) (urging that the Court treat challenges to government surveillance as presenting cognizable claims under political process theory).

I. UNDERSTANDING THE USA FREEDOM ACT AND EXECUTIVE ORDER 12333

In June 2013, Edward Snowden made worldwide headlines when he revealed that the NSA had implemented sweeping surveillance of Americans under Section 215 of the Patriot Act.[39] That month, *The Guardian* published a top secret order from the FISC directing a major U.S. telephone company to turn over to the NSA, on a daily basis, millions of its customers' call records.[40] The order, leaked by Snowden, compelled Verizon to deliver to the NSA the telephony metadata relating to all domestic calls, as well as all calls with one end in the United States, for a three-month period.[41] Within weeks, the government was forced to admit not only the program's continued existence, but also that it been first approved by the FISC in 2006, that similar FISC orders had been issued to other major American telecommunications providers, and that those orders had been continually reauthorized.[42] The result was instant notoriety for Snowden, shock and disbelief on the part of many Americans, and the standard invocation of terrorism prevention as a justification by the Obama Administration.[43] Metadata, once a term familiar only to information technologists and data analysts, entered the standard American vocabulary.

Following the Snowden disclosures, Congress seemed eager to pass legislation to curb the NSA's ability to spy on Americans; more than twenty bills were introduced for the purpose of limiting NSA surveillance powers.[44] It took until June 2015, however, for the Freedom Act to become law—two days after Section 215 technically had

---

39 *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

40 *The Guardian* published the full text of the FISC order. *See Verizon Forced to Turn Over Telephone Data—Full Court Ruling*, THE GUARDIAN, June 5, 2013, http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

41 *Id.*

42 *See* Letter from James R. Clapper, Dir. of Nat'l Intelligence, to Sen. Ron Wyden, http://www.wyden.senate.gov/download/?*id*=285dc9e7-195a-4467-b0fe-caa857fc4e0d&download=1; ADMIN. WHITE PAPER, *supra* note 29, at 2.

43 ADMIN. WHITE PAPER, *supra* note 29, at 3 (stating that telephony metadata collection program was designed to "close critical intelligence gaps that were highlighted by the September 11, 2001 attacks.").

44 Ryan Gallagher, *U.S. Lawmakers Launch Assault on NSA Domestic Snooping*, SLATE (Oct. 29, 2013), http://www.slate.com/blogs/future_tense/2013/10/29/sensenbrenner_and_leahy_s_usa_freedom_act_seeks_to_curb_nsa_domestic_spying.html.

expired.[45] In this Part, I briefly outline the provisions of the Freedom Act, and contrast them with what we know about government's ability to collect and analyze communications metadata under EO 12333.

A. The USA Freedom Act

Of the various surveillance bills introduced in Congress, the original 2013 version of the Freedom Act was considered to be among the most comprehensive.[46] However, by the end of 2014, the House had significantly weakened the bill's privacy protections, and the bill stalled in the Senate.[47] In April 2015, with Section 215's May 31 sunset date looming, legislators introduced a revised version of the Freedom Act in the House and Senate judiciary committees.[48] Despite fervent opposition by both reformers and surveillance hawks in the Senate, this version ultimately won congressional approval and was signed by the President.[49]

Effective 180 days after its enactment, the Freedom Act forbids the government from indiscriminately collecting telephony metadata in bulk under Section 215.[50] As of November 29, 2015, the Freedom Act established a new framework under which call detail records will remain with the telecommunications companies.[51] If the government can demonstrate a reasonable, articulable suspicion that a "specific selection term"—i.e. a person's name or account number—is associated with international terrorism, the FISC may issue an order requir-

45 When the Senate in a rare Sunday session failed to reauthorize or reform Section 215 before its sunset date, intelligence officials said they shut the telephony metadata program down for the first time in fourteen years. *See* Lisa Mascaro, *NSA Bulk Collection of Phone Data Stops; Senate Fails to Act Before Deadline*, L.A. TIMES (May 31, 2015), http://www.latimes.com/nation/politics/politicsnow/la-na-senate-nsa-20150531-story.html#page=1. The Freedom Act restored the government's ability to operate the former Section 215 program for six months while the government and telecommunications providers transition to the new system. Freedom Act, *supra* note 4, at § 109(a).

46 *See* Gallagher, *supra* note 44.

47 Charlie Savage & Jeremy W. Peters, *Move to Restrict Data Collection Blocked G.O.P.*, N.Y. TIMES, Nov. 19, 2014, at A1, A15.

48 Spencer Ackerman, *NSA Reform Bill Imperilled as it Competes with Alternative Effort in the Senate*, THE GUARDIAN (Apr. 28, 2015), http://www.theguardian.com/us-news/2015/apr/28/house-nsa-reform-bill-senate-usa-freedom-act.

49 Jennifer Steinhauer & Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 Is Sharply Limited*, N.Y. TIMES, June 3, 2015, at A1.

50 Freedom Act, *supra* note 4, at §§ 103, 109(a).

51 For a discussion of whether having the private sector keep domestic telephony metadata reduces or increases the risks to individual privacy, see David E. Pozen, *Privacy-Privacy Trade-Offs*, 83 U. CHI. L. REV. (forthcoming 2015) ("[K]eeping the metadata with the private sector or with some newly created entity might merely shift the locus and expand the scope of the privacy threat, at least if the implementing rules are not well designed.").

ing the phone companies to produce, on an ongoing, daily basis, call records within two degrees of separation from the selection term.[52] (The first "hop" worth of call records includes all calls made by or to the suspect number. A second "hop" would provide the NSA with records of all calls made or received by each number identified in the first "hop.") Ongoing production orders are limited to 180 days, although, as before, those orders can be extended with FISC approval.[53] Additionally, the Freedom Act requires the government to promptly destroy all call detail records determined to be irrelevant to foreign intelligence,[54] and allows FISC judges to impose additional minimization procedures to protect nonpublic information concerning U.S. persons.[55]

Under Title II of the Freedom Act, the government is foreclosed from using the pen register/trap and trace provisions of the Patriot Act[56] as an alternate means to implement bulk metadata collection. Section 201 of the Freedom Act provides that the government may only apply for a pen register or trap and trace device on the basis of a "specific selection term," which is defined to exclude broad terms such as zip codes, or the names of cities or computing services.[57] This provision is particularly important because the NSA relied on the Patriot Act pen register/trap and trace provisions as authority to collect a huge amount of domestic email metadata from 2004 to 2011.[58] Title V of the Freedom Act limits the national security letter program in the same fashion, prohibiting the government from obtaining a national security letter[59] except upon application based on a specific identifier.[60]

---

52 Freedom Act, *supra* note 4, at § 101.

53 *Id.*

54 *Id.*

55 *Id.* at § 104(a)(3).

56 *Id.* at §§ 201–02. In the pre-Patriot Act era, a pen register was a device that recorded the numbers dialed from a particular phone, and a trap and trace device recorded the numbers of incoming calls received by a particular phone. The Patriot Act amended FISA to expand these definitions to include devices that capture the dialing, routing, addressing, or signaling information related to electronic and Internet communications, as well as standard telephone calls. Patriot Act, *supra* note 6, at § 214.

57 Freedom Act, *supra* note 4, at § 201.

58 The FISC authorized the email metadata program even though it involved the collection of "an enormous volume of communications, the large majority of which will be unrelated to international terrorism" and that would include "communications of United States persons located within the United States who are not the subject of any FBI investigation." *See* Kollar-Kotelly Opinion, *supra* note 25, at 28, 39. For a more detailed description of this program, see PCLOB Section 215 Report, *supra* note 7, at 38–40.

59 National security letters, which are authorized under four federal statutes, are written directives by which the FBI can compel telephone companies, Internet service providers,

Title VI imposes detailed disclosure and reporting requirements on the government regarding the extent of surveillance activities under FISA. Under Section 601 of the Freedom Act, the Attorney General must provide an expanded annual report to Congress that includes the total number of applications made, granted, and denied for daily production of call detail records under the new framework described above.[61] Furthermore, the DNI must furnish an annual report to the public identifying, among other things, the total number of FISA court orders issued for electronic surveillance, call detail records, and pen registers and trap and trace devices, as well as a good faith estimate of the number of targets of those orders.[62] Finally, Title VII of the Freedom Act provides that the new surveillance framework remains in effect until December 15, 2019.[63]

While the Freedom Act's supporters hailed the new law as a historic limitation on the government's surveillance powers as well as a restoration of Americans' privacy rights,[64] others had a less sanguine response to the statute, noting that the reforms are actually quite modest.[65] The Freedom Act curtails the NSA's ability to gather all our phone metadata under Section 215, but does not terminate the program, which is why many privacy and civil liberties advocates, including both the ACLU and the Tea Party, had called for Congress to allow the provision to expire altogether.[66] Although the government

---

banks, credit agencies, and other institutions to produce records about their customers. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF PROGRESS IN IMPLEMENTING RECOMMENDATIONS AND EXAMINATION OF USE IN 2007 THROUGH 2009, at 2–3 (Aug. 2014).

60 Freedom Act, *supra* note 4, at § 501.

61 *Id.* at § 601.

62 *Id.* at § 602–03.

63 *Id.* at § 705.

64 *See, e.g.*, Press Release, Sen. Patrick Leahy, Senate Passes Historic Lee-Leahy USA Freedom Act (June 2, 2015), http://www.leahy.senate.gov/press/senate-passes-historic-lee-leahy-usa-freedom-act (stating that the Freedom Act will enact the most significant reforms to government since the Patriot Act and it will help to ensure the privacy rights of all Americans).

65 *See, e.g.*, Kelly, *supra* note 11 (quoting ACLU representative that Freedom Act failed to achieve "comprehensive reform"); Sam Sacks, *USA Freedom Act Passes House, Codifying Bulk Collection for First Time, Critics Say*, THE INTERCEPT (May 13, 2015), https://firstlook.org/theintercept/2015/05/13/usa-freedom-act/ (noting statements by House Representatives who voted against the Freedom Act because they believed it did not go far enough to protect civil liberties).

66 *See* John Hudson, *Tea Party and ACLU Call on Congress to let Patriot Act Expire*, FOREIGN POLICY (May 29, 2015), http://foreignpolicy.com/2015/05/29/tea-party-and-aclu-call-on-congress-to-let-patriot-act-expire/ ("In an extreme case of strange bedfellows, a top Tea Party group and the American Civil Liberties Union are pressing lawmakers to allow the

will no longer store all our telephony metadata, it will be able to access the same two-hops worth of metadata authorized under the former Section 215 program,[67] an amount that a former NSA-analyst-turned-whistleblower has estimated could provide the government with billions of call records.[68] Indeed, the Office of the Director of National Security stated in November 2015 that "the overall volume of call detail records subject to query pursuant to court order is greater under [the] USA FREEDOM ACT" than under the former Section 215 program.[69]

Even more importantly, the Freedom Act does not curtail the government's power to collect communications metadata under other laws such as EO 12333, discussed below. In this regard, statements made by members of the intelligence community after passage of the Freedom Act were telling. Less than two weeks after the Freedom Act was signed into law, former NSA Director General Michael Hayden indicated that Congress had let the NSA get off easy:

> If somebody would come up to me and say, "Look, Hayden, here's the thing: This Snowden thing is going to be a nightmare for you guys for about two years. And when we get all done with it, what you're going to be required to do is that little 215 program about American telephony metadata—and, by the way, you can still have access to it, but you got to go to the court and get access to it from the companies, rather than keep it to yourself"—I go: "And this is it after two years? Cool!"[70]

Given that the Freedom Act merely limits what General Hayden described as "that little 215 program" while it allows the government's metadata collection activities to continue under other laws, it is unsurprising that a former senior intelligence official referred to the

---

controversial provisions of the Patriot Act that authorize the National Security Agency's broad surveillance activities to expire.").

67 The FISC originally authorized the NSA to gather phone records that were three "hops" removed from the original seed identifier. *See* ADMIN. WHITE PAPER, *supra* note 29, at 3–4 (stating that under the FISC's order, the NSA may also obtain information concerning second and third-tier contacts of the identifier). In January 2014, President Obama indicated that going forward, the NSA would limit its contact chaining to two "hops." *See* Mark Landler & Charlie Savage, *Obama Outlines Calibrated Curbs on Phone Spying*, N.Y. TIMES, Jan. 18, 2014, at A6.

68 *See* Steven Nelson, *NSA Whistleblowers Oppose Freedom Act, Endorse Long-Shot Bill*, U.S. NEWS & WORLD REP. (Apr. 27, 2015), http://www.usnews.com/news/articles/2015/04/27/nsa-whistleblowers-oppose-freedom-act-endorse-long-shot-bill.

69 *See* Office of the Dir. of Nat'l Intelligence, Fact Sheet: Implementation of the USA FREEDOM ACT of 2015, 3 (2015), http://www.dni.gov/files/icotr/USAFA%20Implementation%20Fact%20Sheet.pdf.

70 Dan Froomkin, *Hayden Mocks Extent of Post-Snowden Reform: "And This is it After Two Years? Cool!"*, THE INTERCEPT (June 17, 2015), https://firstlook.org/theintercept/2015/06/17/hayden-mocks-extent-post-snowden-surveillance-reform-2-years-cool/.

Freedom Act's passage as "a big win for the NSA, and a huge nothing burger for the privacy community."[71]

B. Executive Order 12333

Compare the Section 215 domestic metadata collection program as limited by the Freedom Act with foreign data collection conducted pursuant to EO 12333.[72] EO 12333 provides the framework under which the nation's intelligence agencies engage in foreign intelligence gathering. Issued by President Reagan in 1981, this little-known executive order (referred to as "twelve-triple-three") is considered by the NSA to be the "foundational authority" pursuant to which it collects, retains, analyzes, and disseminates signals intelligence information.[73] To the extent that the NSA's intelligence-gathering activities fall outside the scope of FISA, those activities are governed by EO 12333 and have not been subject to judicial review or significant Congressional oversight.[74] Electronic surveillance conducted under EO 12333 reportedly is huge; NSA data collection under its auspices is said to dwarf that gathered under the former Section 215 telephony metadata program or any other FISA authority.[75] For example, the *Washington Post* reported in 2013 that under EO 12333, the NSA had infiltrated the fiber optic connections that link Yahoo and Google's

71 Shane Harris, *'Big Win' for Big Brother: NSA Celebrates the Bill That's Designed to Cuff Them*, DAILYBEAST (May 14, 2015), http://www.thedailybeast.com/articles/2015/05/14/nsa-loves-the-nothing-burger-spying-reform-bill.html.

72 EO 12333, *supra* note 13.

73 *See* NSA Memorandum, *supra* note 14, at 2. The NSA defines "signals intelligence" as "intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems." Nat'l Sec. Agency Cent. Sec. Serv., Signals Intelligence, www.nsa.gov/sigint/ (last visited Sept. 25, 2015).

74 *See* NSA Memorandum, *supra* note 14, at 2; *see also* Margo Schlanger, *Intelligence Legalism and the Nat'l Sec. Agency's Civil Liberties Gap*, 6 HARV. NAT'L SEC. J. 112, 130 (2015) ("For the wide swathes of foreign intelligence surveillance that are not covered by FISA, regulation under Executive Order 12,333 occurs without judicial involvement."); Ali Watkins, *Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued*, MCCLATCHY DC (Nov. 21, 2013), http://www.mcclatchydc.com/news/nation-world/national/national-security/article24759289.html (quoting Sen. Dianne Feinstein that Senate Intelligence Committee has not been able to oversee EO 12333 surveillance programs "sufficiently" because "they are under the executive branch entirely").

75 *See* Nat'l Sec. Admin.: Hearing Before the S. Comm. on the Judiciary, 113 Cong. 1 (2013) (opening statement of Keith B. Alexander, Dir., NSA), http://www.judiciary.senate.gov/imo/media/doc/10-2-13AlexanderTestimony.pdf (stating that the NSA conducts most of its intelligence activities "solely pursuant to the authorities provided by Executive Order 12333"); Watkins, *supra* note 74.

overseas data centers, which allowed the agency to collect more than 181 million communications records in a one-month period.[76]

In a nutshell, EO 12333 authorizes the government to engage in electronic surveillance from abroad for foreign intelligence purposes. Specifically, Section 2.3(c) allows intelligence agencies to collect, retain, and disseminate data regarding U.S. persons that is obtained as part of a lawful foreign intelligence investigation.[77] Under FISA, the NSA may not intentionally target a U.S. person's foreign communications without obtaining a FISA warrant.[78] However, "vacuum cleaner" collection of communications from abroad is regarded by the NSA as not targeting anyone, which means that the protections of FISA do not apply.[79] Overseas dragnet collections conducted under EO 12333

---

76 *See* Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

77 EO 12333, *supra* note 13, at § 2.3(c). Any collection, retention, or dissemination of U.S. person information must be done in accordance with Attorney General approved procedures. *Id.* at § 2.3.

78 *See* 50 U.S.C. § 1881c(a)(2). Department of Defense procedures implementing EO 12333 also provide that communications of a U.S. person can be intentionally intercepted under EO 12333 if the Attorney General finds probable cause to believe that the person is an agent of a foreign power and that the purpose of the interception is to collect significant foreign intelligence. Nat'l Sec. Agency & Cent. Sec. Serv., Classified Annex to Dept. of Defense Procedures Under Exec. Order 12333 (Mar. 11, 2004) § 4A(1)(4), https://www.aclu.org/files/natsec/nsa/NSA%20Core%20Intelligence%20Oversight%20Training%20Materials.pdf [hereinafter Classified Annex] (Classified Annex starts at p. 118); *see also* Jonathan Mayer, *Executive Order 12333 on American Soil, and Other Tales from the FISA Frontier*, WEB POLICY (Dec. 3, 2014), http://webpolicy.org/2014/12/03/eo-12333-on-american-soil/.

79 *See* NSA Dir. of Civil Liberties and Privacy Office Report, NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333 § 1 n.3 (Oct. 7, 2014) [hereinafter Targeted SIGINT Report] (defining "targeted" signals intelligence (SIGINT) activities under EO 12333 as excluding "bulk" collection of intelligence data that the NSA acquires without the use of specific identifiers); Margo Schlanger, *US Intelligence Reforms Still Allow Plenty of Suspicionless Spying on Americans*, JUST SECURITY (Feb. 13, 2015), http://justsecurity.org/20033/guest-post-intelligence-reforms-plenty-suspicionless-surveillance-americans/ (explaining that FISA does not regulate "(a) *non-targeted* collection of wire communications, including communications between Americans within the US, as long as the actual wire being tapped is located overseas, or (b) *non-targeted* collection of wireless communications if at least one party to the communication is located abroad").

In 2014, President Obama released Presidential Policy Directive 28, which limits the purposes for which U.S. intelligence agencies can engage in bulk collection to detecting and countering threats and activities related to (1) espionage; (2) terrorism; (3) weapons of mass destruction; (4) cybersecurity; (5) the armed services; and (6) transnational crime. Office of the Press Sec'y, Presidential Policy Directive/PPD-28, Signals Intelligence Activities (Jan. 17, 2014) § 2, http://fas.org/irp/offdocs/ppd/ppd-28.pdf [herein-

cannot help but "incidentally" harvest sizeable quantities of U.S. person communications, including, for example, both content and metadata of telephone calls made by Americans to or from a foreign country,[80] or among Americans who happen to be living, traveling, or studying abroad.[81]

These extraterritorial communications are presumed to belong to foreigners[82] who, when situated abroad, lack any Fourth Amendment rights.[83] Considering foreign-collected data to be of foreign provenance made sense in 1981 when EO 12333 was adopted, because domestic and international communications could be differentiated.[84] Back then, phone calls between two Americans traveled over phone lines located solely inside the United States, and therefore could not be swept up as part of the government's foreign surveillance activities. Today, however, even purely domestic communications often travel

---

after PPD-28]. It further states that "in no event may signals intelligence collected in bulk be used for the purpose of suppressing or burdening criticism or dissent." *Id.* However, the directive also provides that these limits on bulk collection "do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection." *Id.* at § 2 n.5. It is unclear whether metadata gathered under EO 12333 would be considered a "collection" under PPD-28. *See infra* notes 105–09 and accompanying text.

80 *See* NSA Memorandum, *supra* note 14, at 2 ("To the extent a person located outside the United States communicates with someone inside the United States or someone inside the United States communicates with a person located outside the United States those communications could also be collected [under EO 12333].").

81 *See* Barton Gellman & Ashkan Soltani, *NSA Records Calls of an Entire Nation*, WASH. POST, Mar. 19, 2014, A1, A16, https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html (describing NSA voice interception program that monitors and records every phone call made within a specified country, which also "pulls in a great deal of content from Americans who telephone, visit and work in the target country"); Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST (Dec. 4, 2013), http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html [hereinafter Gellman & Soltani, *NSA Tracking*] (quoting NSA officials confirming that the agency "incidentally" obtains location data from American cell phones when it taps into the cables that connect mobile networks around the world, and when Americans use their cell phones when they travel outside the United States).

82 For the purposes of EO 12333, "foreign communication" is defined as "a communication that involves a sender or an intended recipient who is outside the United States or that is entirely among foreign powers or between a foreign power and officials of a foreign power." Classified Annex, *supra* note 78, at § 2. *See also* Axel Arnbak & Sharon Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad*, 21 MICH. TELECOMM. & TECH. L. REV. 317, 321–22, 335 (2015).

83 See United States v. Verdugo-Urquidez, 494 U.S. 259, 261 (1990).

84 For an explanation and thoughtful critique of the notion of territoriality and the Fourth Amendment when applied to electronic data in general, and with respect to EO 12333 in particular, see Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326 (2015).

over international cables or are stored on backup servers located in foreign countries, where they are fair game for bulk collection meant to detect or counter terrorism.[85]

This means that the NSA is free to leverage the global nature of our communications networks to harvest communications that, in the pre-digital era, would have been wholly domestic in character. A former NSA chief analyst told the *Washington Post* in 2013 that the NSA prefers to avoid legal restrictions on data collection whenever possible. "Look, NSA has platoons of lawyers, and their entire job is figuring out how to stay within the law and maximize collection by exploiting every loophole," the former analyst said. "It's fair to say the rules are less restrictive under Executive Order 12333 than they are under FISA."[86] In fact, scholars have identified how the NSA could, if it so desired, deliberately use Internet network protocols to route American domestic network traffic abroad in order to scoop it up under EO 12333, thereby evading Fourth Amendment limitations and FISA procedures.[87] (Whether the NSA would actually use these tactics is, of course, only a matter of speculation.)[88]

Although EO 12333 specifically allows intelligence agencies to collect, retain, and disseminate data on U.S. persons as part of lawful foreign intelligence operations,[89] it also directs those agencies to "use the least intrusive techniques feasible within the United States or directed against United States persons abroad."[90] Accordingly, the NSA must comply with AG-approved procedures for handling U.S. person

85 *See* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 183 (Dec. 2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [hereinafter PRG REPORT] (explaining that "[e]ven for a person in the US who never knowingly sends communications abroad, there may be collection by US intelligence agencies outside of the US" under EO 12333); *see also* Gellman & Soltani, *supra* note 76, (explaining how EO 12333 allows the NSA to intercept and collect vast numbers of communication records from overseas data centers); Ellen Nakashima & Ashkan Soltani, *Privacy Watchdog's Next Target: the Least-Known but Biggest Aspect of NSA Surveillance*, WASH. POST (July 23, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/07/23/privacy-watchdogs-next-target-the-least-known-but-biggest-aspect-of-nsa-surveillance (describing how Americans' communications transit across national borders and are often stored overseas).

86 Gellman & Soltani, *supra* note 76.

87 *See* Arnbak & Goldberg, *supra* note 82, at 343–56.

88 The NSA responded to this suggestion by noting that the NSA must procure a FISA warrant to target any U.S. person for electronic surveillance, except in certain limited situations. *Id.* at 339. As the article authors note, however, this answer fails to respond to their concerns regarding untargeted, bulk network collection. *Id.* at 339–40.

89 EO 12333, *supra* note 13, at § 2.3(c).

90 *Id.* at § 2.4.

information acquired under EO 12333.[91] Those procedures, however, are much more privacy protective with respect to communications content as opposed to communications metadata. For example, NSA personnel are directed to make "every reasonable effort, through surveys and technical means, to reduce to the maximum extent possible" any incidental collection of the content of domestic communications under EO 12333.[92] While EO 12333 content-minimization requirements are not as stringent as those imposed on U.S. person communications collected incidentally or inadvertently under Section 702 of FISA,[93] they at least provide some privacy protections with respect to the contents of incidentally acquired, domestic communications.

Communications metadata is another matter. Thanks to Edward Snowden, we know that the NSA believes it has practically unlimited ability to analyze and augment Americans' communications metadata gathered under EO 12333, and use it to create large-scale graphs of Americans' social connections. In September 2013, the *New York Times* published internal NSA documents indicating that, beginning in November 2010, the NSA changed its procedures to allow its analysts to contact chain EO 12333 metadata even when that metadata contained American selectors such as phone numbers and email addresses.[94] Prior to that date, the NSA required analysts to stop contact

---

91 *Id.* at § 2.3.

92 *See* Classified Annex, *supra* note 78, at § 3. For a summary of the minimization procedures that apply to communications content collected by the NSA under EO 12333, see NAT'L SEC. AGENCY, LEGAL FACT SHEET: EXECUTIVE ORDER 12333, at 126 (2013), https://www.aclu.org/files/assets/eo12333/NSA/Legal%20Fact%20Sheet%20Executive%20Order%2012333.pdf [hereinafter NSA Legal FACT SHEET].

93 For a thorough overview of surveillance conducted under Section 702 of the FISA Amendments Act, including an explanation of targeting and minimization procedures, see David Medine et al., PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014), https://www.pclob.gov/library/702-Report.pdf [hereinafter PCLOB SECTION 702 REPORT]. According to the PCLOB Section 702 Report, both communication content and metadata collected under Section 702 is considered to be a "communication," and is therefore protected by minimization procedures. *Id.* at 127 n.524.

The NSA's 2014 Section 702 minimization procedures have been publicly released. *See* Nat'l Sec. Agency/Cent. Sec. Serv., Exihibit B: Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (2007), http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf.

94 *See* James Risen & Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. TIMES, Sept. 28, 2013 at A1, http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?_r=0 (linking NSA Contact-Chaining Memo and Example Social Network Graph, documents which have not been declassified or officially acknowledged by the government).

chaining when they bumped up against an American phone number, email address, or other metadata term.[95] A NSA spokeswoman explained that the policy change reflected the Supreme Court's 1979 holding in *Smith v. Maryland* ,[96] that Americans have no reasonable expectation of privacy in, and hence no Fourth Amendment protection of, their phone records.[97] The *Times* also revealed that the NSA enriches EO 12333 metadata by combining it with material from public and commercial databases, GPS location information, Facebook profiles, and other sources.[98] Several days later, then-NSA Director General Keith Alexander confirmed many of the article's claims while testifying before the Senate Judiciary Committee. [99]

The subsequently declassified NSA procedures described by the *Times* were approved by Attorney General Michael B. Mukasey in 2008 and are set out in a document entitled "Special Procedures Governing Communications Metadata Analysis" ("SPCMA").[100] Not fully implemented by the NSA until 2010,[101] SPCMA authorizes the agency to conduct contact chaining (and undefined "other" analysis) on all EO 12333-collected communications metadata, limited only by the caveat that such analysis be performed for "valid foreign intelligence purposes."[102] SPCMA imposes no hop limits to cabin the NSA's ability to conduct social network analysis; rather, the NSA's ability to contact chain any EO 12333 telephony or email metadata appears to be infinite:

---

95 *Id.*

96 442 U.S. 735 (1979). *See infra* notes 143–49 and accompanying text.

97 Risen & Poitras, *supra* note 94. The NSA's legal rationale for changing its procedures to allow contact chaining through American identifiers is set out in more detail in a top-secret memorandum that was leaked by Edward Snowden but has not been declassified or officially acknowledged by the government. *See* Memorandum for the Att'y Gen., from Kenneth L. Wainstein, Assistant Att'y Gen., Proposed Amendment to Dept. of Def. Procedures to Permit the Nat'l Sec. Agency to Conduct Analysis of Communications Metadata Associated with Persons in the United States 4–6 (Nov. 20, 2007), http://www.theguardian.com/world/interactive/2013/jun/27/nsa-data-collection-justice-department [hereinafter Wainstein Memo].

98 Risen & Poitras, *supra* note 94.

99 *Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act: Before the S. Comm. on the Judiciary*, 113th Cong. (2013), http://www.judiciary.senate.gov/meetings/continued-oversight-of-the-foreign-intelligence-surveillance-act (testimony of NSA Director Keith B. Alexander).

100 NAT'L SEC. AGENCY/CENT. SEC. SERV., DEPT. OF DEFENSE SUPPLEMENTAL PROCEDURES GOVERNING COMMUNICATIONS METADATA ANALYSIS (2008) [hereinafter SPCMA], http://www.dni.gov/files/documents/0909/DoD%20Supplemental%20Procedures%202008080314.pdf.

101 *See* Risen & Poitras, *supra* note 94.

102 SPCMA, *supra* note 100, at § 3(a). SPCMA gives no indication what any other additional analysis might be.

> Contact chaining . . . shows, for example, the telephone numbers or e-mail addresses that a particular telephone number or e-mail address has been in contact with, or has attempted to contact. Through this process, computer algorithms automatically identify not only the first tier of contacts made by the seed telephone number or e-mail address, but also the further contacts made by the first tier of telephone numbers or e-mail addresses and so on.[103]

By allowing the NSA to contact chain through American identifiers for an unlimited number of hops, SPCMA theoretically provides the government with a means to acquire comprehensive databases of domestic calls and email records. Nothing in the EO 12333 regime requires the government to limit metadata searches to identifiers for which it has a reasonable articulable suspicion of a link to terrorism; again, a foreign intelligence purpose is enough. And unlike the Freedom Act, which requires the NSA to purge telephony metadata that is irrelevant to foreign intelligence, communications records obtained under EO 12333 may be retained in a government database for at least five years.[104]

With respect to dissemination of U.S. person information that the NSA incidentally acquires under EO 12333, the agency applies the same rules whether the information came from communications content or metadata.[105] However, any privacy protections for U.S. person data contained in the AG-approved procedures implementing EO 12333 do not apply to searches of communications metadata obtained under that order. This is because privacy protections provided by those documents only apply to information that is "collected" under the government's own definition. Understanding how this works requires tracking a convoluted series of definitions contained in various policy directives.

---

103 *Id.* at § 2(b); *see also* SIGNALS INTELLIGENCE DIRECTORATE ("SID") MANAGEMENT DIRECTIVE NO. 424, SIGINT DEVELOPMENT—COMMUNICATIONS METADATA ANALYSIS 3 (2010), https://epic.org/privacy/surveillance/12333/20150312-NSA-production.pdf (exhibit to letter) (stating that for a valid foreign intelligence purpose, communications metadata obtained under EO 12333 may be subject to "complete contact chain analysis").

104 *See* NAT. SEC. AGENCY, ET AL., UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE SP0018, § 6 (2011) [hereinafter USSID 18], http://www.dni.gov/files/documents/1118/CLEANED Final%20USSID%20SP0018.pdf. *See also* Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293, 128 Stat. 3990 (2014), § 309 (requiring intelligence agencies to limit retention to five years of nonpublic telephone or electronic communications to or from a U.S. person that were obtained without a court order, with certain exceptions, including for communications with foreign intelligence value).

105 *See* NSA LEGAL FACT SHEET, *supra* note 92, at 126 (summarizing dissemination standards and explaining that they are the same for metadata and communication content of or concerning U.S. persons).

First, Department of Defense ("DoD") Directive 5240.1-R, which sets out procedures regarding intelligence activities affecting U.S. persons, provides that data acquired electronically is not "collected" until it has been received for use by an intelligence agency and "processed into intelligible form."[106] While the meaning of "intelligible form" is not defined, a further NSA directive explains that information is not "collected" until an NSA analyst intentionally "task[s] or selects" a communication for "subsequent processing aimed at reporting or retention as a file record."[107] Finally, SPCMA amended DoD Directive 5240.1-R to "clarify" that "contact chaining and other metadata analysis do not qualify as 'interception' or 'selection' of communications."[108] In this way, the intelligence community has redefined "collection" to exclude electronic gathering and analysis of communications metadata from otherwise applicable minimization procedures.[109] Remember that these policies and procedures are developed and applied solely within the executive branch without FISC approval, and that Congress has not chosen to subject NSA activities under EO 12333 to significant oversight.[110]

From this discussion, it should be clear why EO 12333 has been described as a legal loophole that allows the NSA to take advantage of our global communications network to justify warrantless surveillance of Americans.[111] In a 2014 *Washington Post* op-ed piece, former State Department official-turned-whistleblower, John Napier Tye, tried to warn Americans about the massive scope of NSA surveillance under EO 12333, suggesting that the former Section 215 telephony metada-

106 U.S. DEP'T OF DEF. DIRECTIVE 5240.1-R, PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS, § C2.2.1 (1982).

107 USSID 18, *supra* note 104, at § 9.2.

108 SPCMA, *supra* note 100, at § 4.

109 For helpful analysis and explanation regarding these definitions and their implications, see Faiza Patel, *How the Second Circuit's Decision in Clapper Informs the Section 215 Discussion*, JUST SECURITY (May 11, 2015), http://justsecurity.org/22944/clapper-section-215-discussion/; *Did the Second Circuit Decision ALSO Blow Up SPCMA?*, EMPTYWHEEL (May 11, 2015), https://www.emptywheel.net/2015/05/11/did-the-second-circuit-decision-also-blow-up-spcma/.

110 According to the Wainstein Memo, the NSA briefed the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence regarding SPCMA sometime prior to Nov. 20, 2007. *See* Wainstein Memo, *supra* note 97, at 3.

111 See John Napier Tye, *Meet Executive Order 12333: The Reagan Rule that Lets the NSA Spy on Americans*, WASH. POST (July 18, 2014), http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html (arguing that EO 12333 contains a legal loophole that allows for U.S. persons' communications "incidentally" collected to be retained, despite the fact that EO 12333 prohibits U.S. persons from being targeted without a court order).

ta program was merely "a mechanism to backfill that portion of U.S. person data that cannot be collected overseas under 12333."[112] Tye also hinted that the NSA still stockpiles U.S person email and other Internet metadata under EO 12333, despite assurances by General Alexander that the FISC-approved program under the pen register/trap and trace provisions of the Patriot Act discussed earlier had been discontinued in 2011 to "better protect civil liberties and privacy."[113] Although the Freedom Act forbids the NSA from using the Patriot Act provisions to restart this program in bulk, again, the new law has no effect on the NSA's activities under EO 12333.[114]

To recap, many Americans were outraged to learn in 2013 that the NSA, with FISC approval, was collecting and analyzing their call detail records without their knowledge or consent under the former Section 215 of the Patriot Act. After two years of debate, Congress imposed some additional limits on the government's ability to collect and scrutinize our telephone or email metadata by enacting the Freedom Act. Some believe these changes are significant; others have been more critical. Congressional reforms to FISA and the Patriot Act, however, are futile if the government can simply continue to gather and analyze our communications metadata as before via an alternate path. Under EO 12333, the NSA can vacuum up domestic communications metadata in bulk as long as the capture occurs from a foreign source or the communications involve one communicant in a foreign country. The NSA is then free to augment that metadata with other information and map the social connections of American citizens, out to an unlimited number of hops, for foreign intelligence purposes. The NSA claims these actions are compatible with the Fourth Amendment because Americans have no reasonable expectation of privacy in their communications metadata. In the next Part, I focus on how communications privacy developed under the Fourth

112 *Id.* Edward Snowden has described EO 12333 as "what the NSA uses when the other [legal] authorities aren't aggressive enough or aren't catching as much [data] as they'd like." Chris Morran, *John Oliver Gets Edward Snowden to Explain Government Snooping in Terms of Penis Photos*, CONSUMERIST (Apr. 6, 2015), http://consumerist.com/2015/04/06/john-oliver-gets-edward-snowden-to-explain-government-snooping-in-terms-of-penis-photos/.

113 Tye, *supra* note 111 (noting that Alexander said only that the NSA stopped collecting this data under the Patriot Act, not that it did not collect the data at all).

114 The NSA admitted as much in November 2015, when it released an inspector general's report confirming that the Patriot Act email dragnet had been shut down in part because the same domestic Internet metadata could be collected abroad under EO 12333 and analyzed pursuant to SPCMA. *See* Charlie Savage, *File Says N.S.A. Found Way to Replace Email Program*, N.Y. TIMES (Nov. 19, 2015), http://www.nytimes.com/2015/11/20/us/politics/records-show-email-analysis-continued-after-nsa-program-ended.html?_r=0.

Amendment, rather than the First, and consider whether *Smith v. Maryland*[115] justifies the NSA's almost-unlimited ability to collect and analyze domestic communications metadata under EO 12333.

II. COMMUNICATIONS METADATA AND THE FOURTH AMENDMENT

Following the Snowden revelations, former President Jimmy Carter famously remarked that he assumes the NSA monitors his electronic communications; accordingly, when he desires to correspond privately with foreign leaders, he writes a letter and posts it in the U.S. mail.[116] Assuming President Carter seeks to shield only the contents of his snail mail, his approach is sound: the Supreme Court first recognized a right to communications privacy in the context of sealed letters. However, the names and addresses of the former president's correspondents, as well as postmarks or other envelope notations—in effect, the communications metadata associated with those letters—can, and well may, be collected by the government without triggering the Fourth Amendment warrant requirement.[117] In this Part, I trace how the Court grounded communications privacy in the Fourth Amendment, rather than the First, and how it developed the third party doctrine in the context of telephone call detail records. Although this is well-travelled territory, I set out these familiar precedents to show how they form the basis for the government's constitutional argument justifying today's bulk metadata surveillance programs.

A. Mail Privacy and the Fourth Amendment Path

Somewhat surprisingly, the protection of communications privacy in America originated not from judicial interpretations of the Constitution, but rather from early postal policies.[118] At least in part in re-

115 442 U.S. 735 (1979).

116 David Jackson, *Carter Uses Snail Mail to Evade NSA*, USA TODAY (Mar. 24, 2014), http://www.usatoday.com/story/theoval/2014/03/24/obama-jimmy-carter-national-security-agency-surveillance-snail-mail/6818605/.

117 In July 2013, *The New York Times* revealed the existence of the Mail Isolation Control and Tracking program, under which U.S. Postal Service computers photograph the outside of every piece of mail processed in the United States, thereby providing the government with a record of mail metadata. *See* Ron Nixon, *U.S. Postal Service Logging All Mail for Law Enforcement*, N.Y. TIMES (July 3, 2013), http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html.

118 *See* Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 557 (2007) ("[A]s a historical matter, it was the post office—

sponse to a history of British postal surveillance,[119] Congress in 1792 enacted the Postal Service Act, which made it a crime for postal officials to open sealed letters unless they were undeliverable.[120] This early postal policy, still reflected in the law today,[121] created public confidence in the sanctity of the mails as well as a public expectation regarding communications privacy, and helped build what Professor Jack Balkin has termed an "infrastructure of free expression"[122] in the new country.

The Supreme Court first considered a claim of communications privacy in *Ex parte Jackson*,[123] an 1878 case where the petitioner relied on the First Amendment to challenge his conviction under a federal law prohibiting all lottery advertisements, even those for legal lotteries, from the mail. Petitioner's counsel argued that the law constituted content-based censorship, which, if allowed, would empower Congress to exclude from the mail communications on any topic it found objectionable.[124] Justice Stephen Field, writing for a unanimous Court, upheld the constitutionality of the statute as a valid exercise of Congress's power to prohibit materials that "have a demoralizing influence upon the people"[125] from the mails; he did not directly address the petitioner's specific First Amendment claim.[126] Rather, Justice Field, in dicta, located privacy protection for letters and sealed packages in the Fourth Amendment, drawing a distinction between "what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined."[127]

Hence, sealed, first-class letters deposited in the U.S. mail for delivery became the sender's papers for the purposes of the Fourth

---

not the Fourth Amendment of its own independent force—that originally gave us the notion of communications privacy that we now view as an abstract constitutional principle applicable to telephone conversations, e-mails, and the like.").

119 *Id.* at 560–65.

120 Act of Feb. 20, 1792, §§ 16, 18, 1 Stat. 232, 236–37.

121 *See* 18 U.S.C. § 1703 (2000) (outlining the misdemeanor offense for a Postal Service officer or employee who unlawfully destroys, delays, or opens mail).

122 Jack M. Balkin, *The First Amendment is an Information Policy*, 41 HOFSTRA L. REV. 1, 3–4 (2012).

123 96 U.S. 727 (1877).

124 *Id.* at 730–31.

125 *Id.* at 736.

126 Justice Field did, however, recognize that mail regulations excluding certain publications from the mail could deliver a "fatal blow" to the First Amendment's guarantee of a free press. *Id.* at 733, 735.

127 *Id.* at 733.

Amendment; their contents (as opposed to "what is open to inspection," such as any envelope notations that could be viewed by all) were not subject to inspection in transit without a warrant. Although the Court could have upheld the statute on First Amendment grounds pursuant to the bad tendency test then used to evaluate speech restrictions,[128] the Court declined to do so. Today, the statute most certainly would be invalid as an unconstitutional restriction of commercial speech, but in 1878, First Amendment protection for advertising was almost a hundred years away.[129] Rather, in an example of path dependency,[130] *Ex parte Jackson* situated the Court's communications privacy analysis in the Fourth Amendment, where it has remained.

B. Electronic Eavesdropping and False Friends

The advent of electronic communications posed two related questions for the Court: are conversations—spoken words—covered by the Fourth Amendment's guarantee against unreasonable search and seizure; and, if so, may the government use electronic means to intercept those words? By the mid-twentieth century, the Court had established that oral statements, as well as papers and effects, fall within Fourth Amendment protections.[131] With respect to government wiretapping, the Court in the landmark 1967 case of *Katz v. United States* drew a distinction between what a person "knowingly exposes to the public" and what he or she "seeks to preserve as private, even in an area accessible to the public," holding that the Fourth Amendment

128 The Court remarked that the statute merely prohibited "corrupting publications and articles" about lotteries—"institutions which are supposed to have a demoralizing influence upon the people." *Id.* at 736. Regarding the "bad tendency" test, see DAVID M. RABBAN, FREE SPEECH IN ITS FORGOTTEN YEARS 132 (1997) ("The most pervasive and fundamental judicial approach to free speech issues between the Civil War and World War I used the bad tendency test derived from Sir William Blackstone's *Commentaries* on the English common law in the eighteenth century.").

129 *See* Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748 (1976); Bigelow v. Virginia, 421 U.S. 809 (1975).

130 By this I mean simply that precedent in a particular area of law may then require, steer, or prohibit the direction of certain choices by the Court in future decisions. *See* Michael J. Gerhardt, *The Limited Path Dependency of Precedent*, 7 U. PA. J. CONST. L. 903, 905 (2005) (exploring the two prevailing views of precedent in scholarly literature, including path dependency).

131 Hoffa v. United States, 385 U.S. 293, 301 (1966) (citing Silverman v. United States, 365 U.S. 505 (1961) (explaining "the protections of the Fourth Amendment are surely not limited to tangibles, but can extend as well to oral statements")); Wong Sun v. United States, 371 U.S. 471, 485 (1963) (quoting Silverman v. United States, 365 U.S. 505 (1961) (holding "that the Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of 'papers and effects'")).

only protects the latter.[132] The defendant, accordingly, was entitled to exclude the "uninvited ear" of the government from his phone conversations even though they occurred in a public phone booth.[133] Because the government had failed to obtain a warrant, its conduct did not comport with the Fourth Amendment.[134]

The real take-away from *Katz*, however, came from Justice John Marshall Harlan II's concurrence where he articulated the iconic two-part reasonable expectation of privacy test: to show that the government conducted an unreasonable search in violation of the Fourth Amendment, an individual must have "an actual (subjective) expectation of privacy" and that expectation of privacy must be one "that society is prepared to recognize as 'reasonable.'"[135] Within a year, the Court had adopted Justice Harlan's test as the controlling principle from *Katz*,[136] and, critical commentary notwithstanding,[137] courts have applied it ever since. As applied by the Court in later cases, Justice Harlan's reasonable expectation of privacy test turned into a balancing of interests approach where judges consider all the circumstances surrounding a search to determine its reasonableness.[138]

During these same years, the Court also addressed questions of communications privacy in the context of criminal suspects who revealed incriminating information to government agents or informants. In these false friend cases, the Court relied on an assumption of

---

132 389 U.S. 347, 351 (1967).

133 *Id.* at 352.

134 *Id.* at 358–59.

135 *Id.* at 361 (Harlan, J., concurring).

136 *See* Terry v. Ohio, 392 U.S. 1, 9 (1968) ("We have recently held that 'the Fourth Amendment protects people, not places,' *Katz v. United States*, 389 U.S. 347, 351 (1967), and wherever an individual may harbor a reasonable 'expectation of privacy,' *id.*, at 361 (Mr. Justice Harlan, concurring), he is entitled to be free from unreasonable governmental intrusion."); *see also* United States v, Jones, 132 S. Ct. 945, 950 (2012) ("Our later cases have applied the analysis of Justice Harlan's concurrence in [*Katz*], which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.'").

137 The reasonable expectation of privacy test has been roundly criticized for its unpredictable and inconsistent results, as well as for its subjectivity and circularity. *See, e.g.*, Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188 (1979) (describing the *Katz* test as "circular" because an individual's reasonable expectation of privacy will always depend upon "what the legal rule is"); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010) (criticizing the *Katz* test as having "led to a contentious jurisprudence that is riddled with inconsistency and incoherence").

138 *See, e.g.*, Ohio v. Robinette, 519 U.S. 33, 39 (1996) (stating that Fourth Amendment reasonableness "is measured in objective terms by examining the totality of the circumstances"); New Jersey v. T.L.O., 469 U.S. 325, 341 (1985) (concluding that the legality of a warrantless search of a public school student "should depend simply on the reasonableness, under all the circumstances, of the search").

the risk theory to hold that when a suspect exchanges information with a confederate, the suspect has no reasonable expectation that the information will remain private.[139] According to the Court, it would be unreasonable for the suspect in that situation to believe either that (1) the confederate will not share the information with law enforcement in the future; or (2) the confederate is not already working for the government, and may be recording or transmitting the conversation as it occurs.[140]

C. Communications Metadata and the Third Party Doctrine

Having developed the assumption of the risk theory in the false friend cases, the Court next applied it to establish that individuals have no reasonable expectation of privacy in information they share with a third-party service provider. In *United States v. Miller*,[141] the Court cited the false friend cases to hold that a bank depositor assumes the risk that the bank will provide her financial records to the government in response to a subpoena *duces tecum*, even though the depositor may have believed the bank would keep the records confidential.[142] Whereas *Miller* dealt with financial records, the Court in *Smith v. Maryland*[143] applied the assumption of the risk rationale to what today we would call communications metadata—in this case, records of phone numbers dialed by a criminal suspect and held by the telephone company. There, at law enforcement request, a local phone company placed a pen register on a robbery suspect's phone line after the victim reported receiving threatening calls from a man who identified himself as her assailant.[144] When the device revealed that, on the very day it was installed, the suspect called the victim's

139 *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 302 (1966) (explaining "[n]either this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it"); Lewis v. United States, 385 U.S. 206, 211 (1966) (holding the Fourth Amendment is not violated when a "home is converted into a commercial center . . . for purposes of transacting unlawful business" and a government agent enters with an invitation to do business).

140 *See, e.g.*, *Hoffa*, 385 U.S. at 302 (noting that by speaking in front of an informant, the defendant had mistakenly relied on the loyalty of someone he mistook for a friend).

141 425 U.S. 435 (1976).

142 *Id.* at 443. ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence place in the third party will not be betrayed.").

143 442 U.S. 735, 744 (1979).

144 *Id.* at 737.

home number, police obtained a warrant to search the suspect's house.[145] At trial, the suspect relied on *Katz* to argue that all evidence derived from the pen register had been obtained in violation of his Fourth Amendment rights.[146]

The Court disagreed, holding that the placement of a pen register on a telephone phone line did not qualify as a Fourth Amendment search.[147] The Court emphasized the pen register's limited ability to reveal only numbers dialed from a particular phone, not whether a call was completed or what was said by either party.[148] Given that all subscribers know that the phone company keeps records of their calls for billing and other purposes, the Court found it implausible that phone customers could have a reasonable expectation of privacy in those records.[149]

Dissenting, Justice Potter Stewart argued that the call logs did, in fact, contain substantive information. Few telephone customers would consent to have a list of their phone calls made public, Justice Stewart observed, not because the numbers would reveal criminal conduct, but because they "easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[150] In a separate dissent, Justice Thurgood Marshall distinguished the false friend cases as situations where the defendants had chosen whether, and to whom, to confide their secrets; the defendant in *Smith* had no choice but to assume the risk of government surveillance to be able to use his telephone.[151] Justice Marshall recognized that warrantless use of pen registers implicates both Fourth and First Amendment values, noting in particular how government monitoring of call records could chill both political association and freedom of the press.[152]

Almost from the day it was decided, *Smith* has been harshly criticized, both as misapprehending the expectations of privacy that people attach to personal records they must, of necessity, deposit with

145 *Id.*
146 *Id.* at 737–38.
147 *Id.* at 745–46.
148 *Id.* at 741–42.
149 *Id.* at 742–43. It should be noted that the *Smith* holding turned on the Court's evaluation of whether someone who, having revealed his phone calls to the phone company, could reasonably expect those records to be held in confidence—not merely that government capture of non-content information is not a search.
150 *Id.* at 748 (Stewart, J., dissenting).
151 *Id.* at 749–50 (Marshall, J., dissenting).
152 *Id.* at 751.

third parties,[153] and for giving the government an untoward ability to monitor its citizens.[154] Although *Smith* raises serious privacy concerns, the scope of the surveillance upheld in *Smith* was both more targeted and much narrower in scope than bulk metadata collection and analysis conducted under EO 12333.[155] In *Smith*, a simple device was placed on the phone line of one specific, named individual whom police had good reason to suspect. Although the NSA will not reveal the volume of incidental collection of U.S. persons' communications metadata collected under EO 12333,[156] intelligence officials have indicated that the former Section 215 program was diminutive in comparison.[157] Given that bulk collection is, by definition, untargeted, it

153 *See, e.g.*, Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1314–15 (1981) (describing the Court's analysis in *Smith* as "misguided"); Clifford S. Fishman, *Pen Registers and Privacy: Risks, Expectations, and the Nullification of Congressional Intent*, 29 CATH. U. L. REV. 557, 567–74 (1980) (criticizing the Court's factual assumptions and legal analysis in *Smith*); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 40, 66 (2004) (faulting the Court in *Smith* for failing to consider how much privacy the law should grant to information that most individuals would consider to be private); Anita Ramasastry, *Lost in Translation? Data Mining, National Security and the "Adverse Inference" Problem*, 22 SANTA CLARA COMPUTER & HIGH TECH. L. J. 757, 764 (2006) (disputing that individuals give up their expectation of privacy in information they provide to third parties in the course of modern life).

Congress responded to *Smith* by enacting the Pen Register Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 3121–27 (2012)), which requires the government to procure a court order before installing a pen register. This is easier for the government to obtain than a traditional warrant; it need only certify that the use of the pen register is "relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a).

154 *See, e.g.*, Jack Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 19 (2008) (citing *Smith* as an example of how the Court has "debilitated the Fourth Amendment" as a tool to prevent government abuse of power); Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1254–56 (1983) (arguing that in *Smith*, the Court gave the government too much power to collect phone records of those who are not guilty or even suspected of criminal activity).

155 The scope of the surveillance upheld in *Smith* was also much narrower than that conducted by the NSA under the former Section 215 telephony metadata collection program. *See, e.g.*, Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Concerns*, 37 HARV. J.L. & POL'Y, 757, 869–71 (2014) (distinguishing telephony metadata collection program from pen register installation in *Smith*); PCLOB Section 215 Report, *supra* note 7, at 114 (stating that *Smith* "does not provide a good fit" for the Section 215 telephony metadata collection program).

156 *See* Gellman & Soltani, *supra* note 81 (quoting intelligence officials saying that it would be "awkward" or impossible to calculate the number of American cell phones tracked overseas by the NSA).

157 *See generally supra* notes 75–76 and accompanying text. Former State Department official John Napier Tye has stated that the NSA collects "a huge amount of Americans' communications and data" under EO 12333. Timothy B. Lee, *Why the Latest Patriot Act Reform Won't Be Enough To Rein in the NSA*, VOX (June 8, 2015, 2:12 PM), http://www.vox.com/2015/6/7/8741095/patriot-nsa-john-tye.

stands to reason that it would include communication records belonging to many U.S. persons who have no connection to terrorism. Police monitored the *Smith* defendant's phone for no more than two days to see whether he dialed only one specific phone number (the victim's).[158] The NSA has been collecting telephony and email metadata associated with U.S. persons under EO 12333 at least since 2007[159] (and probably long before).[160]

The pen register information provided in *Smith* was also less revealing than bulk metadata collection under EO 12333—the pen register recorded only the numbers dialed from one suspect's phone. Call records collected and analyzed by the NSA under EO 12333 include not only the telephone numbers of calls dialed, but also of those received, as well as the date, time, and duration of the call.[161] Email metadata includes information that appears on the "to," "from," "cc," and "bcc" (although not the "subject") lines, plus the Internet-protocol (IP) address of the computer from which an email was sent, IP address of routers and servers that handled the email transmission, plus login and inbox information if a user accesses a web-based email account.[162] As described in Part I, the NSA relies on the third party doctrine to justify performing contact chaining on communications metadata acquired under EO 12333, obtaining an unlimited number of hops worth of additional records as long as its investigation serves a valid foreign intelligence purpose and keeping those records for at least five years.[163]

Not only is this information much richer than that disclosed by the pen register in *Smith*, the communications metadata we generate every day are also more voluminous than anything a time traveler from the 1970s could possibly imagine. We rely today on various forms of electronic communications to handle everyday tasks and connect with almost anyone, anywhere, at any time in a way that was inconceivable in 1979. At the same time, the investigative tools used

158 442 U.S. 735, 737 (1979).

159 *See* Office of General Counsel, Memorandum for the Deputy Chief of Staff, Sharing of "Raw SIGINT" Through Database Access 4–5 (July 12, 2007) (referring to NSA collection of bulk telephony metadata containing numbers with U.S. area codes, and describing difficulty determining whether email metadata were foreign or domestic).

160 The Drug Enforcement Agency admitted that it used administrative subpoenas to collect telephony records of billions of Americans' calls to foreign countries beginning back in 1992. *See* Brad Heath, *U.S. Secretly Tracked Billions of Calls for Decades*, USA TODAY (Apr. 8, 2015), http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/.

161 *See* SPCMA, *supra* note 100, at § 2.

162 *Id.*

163 *See supra* notes 94–104 and accompanying text.

today by the government to aggregate, track, and analyze communications metadata are markedly more sophisticated than anything available during the *Smith* era.

D. The Future of the Third Party Doctrine

Critics of the third party doctrine found reason to hope for its demise based on the recent case of *United States v. Jones*,[164] where five members of the Court demonstrated a heightened sensitivity to the privacy implications of new technology. The *Jones* Court unanimously held that the government must obtain a warrant to attach a global positioning system device to a car to track its movements for twenty-eight days.[165] The government had argued that the defendant had no reasonable expectation of privacy while driving a car on the public roads, where he could be seen by all.[166] Justice Antonin Scalia, writing for the majority, rejected this approach, concluding that the government had conducted a Fourth Amendment search by intruding onto, and physically occupying, private property to obtain information.[167]

In a concurrence joined by Justices Ruth Bader Ginsburg, Stephen Breyer, and Elena Kagan, Justice Samuel Alito applied the *Katz* formula to conclude that long-term monitoring facilitated by new technology violated the defendant's reasonable expectations of privacy.[168] Justice Alito noted that modern technology has given law enforcement the ability to engage in constant, pervasive monitoring that would have been logistically impossible as well as cost-prohibitive in the pre-digital age.[169] Although he called on legislatures to limit law enforcement use of tracking technology, in the absence of statutory guidelines, Justice Alito concluded that the lengthy monitoring here violated the Fourth Amendment.[170] "For [most] offenses," he wrote, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[171]

In a separate concurrence, Justice Sonia Sotomayor addressed the third party issue head on, and called for its reconsideration in light of

164 132 S. Ct. 945 (2012).
165 *Id.* at 947–49.
166 *Id.* at 950.
167 *Id.* at 949.
168 *Id.* at 964 (Alito, J., concurring).
169 *Id.* at 963–64.
170 *Id.* at 964.
171 *Id.*

modern technology.[172] Describing the doctrine as "ill suited to the digital age," she noted that people today have no choice but to reveal information about themselves in the course of completing their daily tasks.[173] She also recognized the importance of First Amendment values in the Fourth Amendment calculation, noting that government monitoring has a chilling effect on speech and association.[174] Accordingly, Justice Sotomayor said she was unwilling to "assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[175]

Of course, *Jones* did not involve communications metadata and, strictly speaking, left the *Smith* holding unchanged. Nevertheless, taken together, the concurring opinions in *Jones* show that at least five Justices have misgivings about intrusive government surveillance made possible by modern technology. Justice Alito noted a particular concern with the ability of wireless carriers to track, record, and aggregate the location of cell phone users,[176] a type of metadata that has been collected by the NSA in the past.[177] In another recent case, *Riley v. California*,[178] the Court unanimously held that police must obtain a warrant before searching data on an arrestee's cell phone. In his opinion for the Court, Chief Justice John Roberts noted the privacy interests associated with digital devices, observing that cell phones can store much more private information than a person typically would carry in a handbag or wallet.[179] The Chief Justice also focused on cell phone location data, citing Justice Sotomayor's concurrence in *Jones* for the proposition that historic location data can be used to reconstruct a person's minute-by-minute movements, both outside and indoors.[180]

Although these two cases may herald a willingness by the Court to adapt the Fourth Amendment to the digital age, *Smith* has yet to be

172 *Id.* at 957 (Sotomayor, J., concurring).
173 *Id.*
174 *Id.* at 956.
175 *Id.* at 957.
176 *Id.* at 963–64 (Alito, J., concurring).
177 *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.
178 134 S. Ct. 2473, 2495 (2014).
179 *Id.* at 2488–89.
180 *Id.* at 2490.

overruled.[181] Indeed, *Smith* remains the major precedent on which both the government and courts consistently have relied to justify or uphold the bulk collection of communications metadata. Before the passage of the Freedom Act, a handful of challengers contested the constitutionality of the former Section 215 telephony metadata program in court, but only one district court judge suggested that it likely violated the Fourth Amendment—a holding later reversed on standing grounds by the D.C. Circuit.[182] The other courts that reached the constitutional question applied *Smith* to hold that phone subscribers have no reasonable expectation of privacy in call detail records shared with their telecommunications providers.[183]

The FISC, as well, has repeatedly invoked *Smith* and the third party doctrine to reauthorize telephony metadata collection under the former Section 215.[184] For example, in a post-*Jones* decision, FISC Judge Eagan cited *Smith* (with no mention of *Jones*) to approve the program, despite its bulk nature. "[W]here one individual does not have a Fourth Amendment interest," she wrote, "grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*."[185] More recently, the FISC again applied *Smith* to deny a constitutional challenge to the Freedom Act's 180-day extension of the former Section 215 program, stating that with regard to the nature of the data

---

181 In *Riley*, Chief Justice Roberts warned in a footnote not to read too much into a decision that did not address "whether the collection or inspection of aggregated digital information amounts to a search under other circumstances." *Id.* at 2489–90 n.1.

182 *See* Klayman v. Obama, 957 F. Supp. 2d 1, 32–42 (D.D.C. 2013), *rev'd*, 800 F.3d 559 (D.C. Cir. 2015) (distinguishing *Smith* to find that citizens have a reasonable expectation of privacy in their telephony metadata, and enjoining the NSA telephony metadata collection program as a likely violation of the Fourth Amendment).

In 2015, the Second Circuit held that the NSA telephony metadata collection program revealed by Edward Snowden exceeded the statutory authority provided to the government under the former Section 215 of the Patriot Act. ACLU v. Clapper, 785 F. 3d 787 (2d Cir. 2015). While the court did not reach the challengers' Fourth Amendment claims, it described those constitutional claims as both "vexing," *id.* at 821, and "daunting," *id.* at 825.

183 *See* Smith v. Obama, 24 F. Supp. 3d 1005, 1007 (D. Idaho 2014); ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *rev'd on other grounds*, 785 F.3d 787 (2d Cir. 2015); United States v. Moalin, No. 10cr4246 JM, 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013).

184 *See* Opinion and Order, In Re Appl. of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things (No. BR 15-75) and In Re Motion in Opp'n to Government's Request to Resume Bulk Data Collection Under Patriot Act Section 215 (No. 15-01), at 12-13 (FISA Ct. June 29, 2015), http://www.fisc.uscourts.gov/sites/default/files/BR%2015-75%20Misc%2015-01%20Opinion%20and%20Order.pdf [hereinafter Mosman opinion] (listing FISC opinions upholding telephony metadata program under Fourth Amendment).

185 Eagan opinion, *supra* note 25, at 9.

acquired, the NSA's bulk collection of Americans' call detail records is "indistinguishable" from the pen register information gathered in the 1979 case.[186]

While one can disagree with the FISC's conclusions, at least government surveillance programs authorized under FISA are subject to some type of court approval. No similar opportunity for FISC review exists with respect to surveillance conducted under EO 12333. Individual Fourth Amendment challenges to EO 12333 bulk metadata collection are highly unlikely to be heard in court at all, given that, absent another Edward Snowden, a litigant will be hard-pressed to demonstrate that his or her communications metadata have been gathered or analyzed under the top-secret program.[187] Still, the constitutional validity of the third party doctrine remains critical because—as discussed in Part I—the NSA relies on *Smith* to justify not only bulk collections, but also limitless contact chaining of communications metadata that the agency knows belong to or are associated with U.S. persons.[188]

If, thanks to *Smith*, the Fourth Amendment fails adequately to protect the privacy of our communications metadata, can we avoid the third party doctrine altogether by looking to the First Amendment for relief? The next Part examines why, despite the free speech implications of communications privacy, First Amendment challenges to bulk communications metadata collection programs are even more likely to fail than those based on the Fourth.

III. COMMUNICATIONS PRIVACY AND THE FIRST AMENDMENT

If the privacy interests of ordinary, law-abiding Americans in their communications records are inadequately protected from incidental collection by the Fourth Amendment thanks to *Smith v. Maryland*[189] and the third party doctrine,[190] can a case be made that bulk collection of communications metadata by the government violates the First Amendment? After all, our ability to contact whomever we

186 Mosman opinion, *supra* note 184, at 19.

187 Standing doctrine provides that litigants cannot bring constitutional challenges without demonstrating that they have suffered an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." Monsanto Co. v. Geertson Seed Farms, 130 S. Ct. 2743, 2752 (2010) (citing Horne v. Flores, 557 U.S. 433, 445 (2009)). *See infra* notes 280–98 and accompanying text.

188 *See supra* notes 94–104 and accompanying text.

189 442 U.S. 735 (1979).

190 *See supra* text accompanying notes 141–86.

please (including family and friends who live abroad) without concurrently notifying Big Brother would seem to be part of our freedom of speech that the government may not abridge. People use email and the telephone to arrange meetings and make plans; to order and inquire about products and services; to ask, answer, and discuss questions regarding personal, political, religious, and professional matters; to seek and offer information and advice; and to share news, thoughts, feelings, opinions, and beliefs with others. If communications metadata is so revealing that the NSA, under EO 12333, taps Internet cables to collect it in hopes of someday identifying possible terrorists and their accomplices, must that metadata not also be revealing enough to implicate the First Amendment?

Scholars have often called for recognition of a First Amendment right to object to government surveillance. Professor Jack Balkin, for example, has warned of the threat to free speech posed by what he calls "new school censorship"—when the government inserts backdoors and surveillance technologies into privately owned communication networks, which then provide the government with the ability to access our digital lives.[191] Professor Neil Richards has argued that government surveillance poses a threat to First Amendment freedom of thought and private consultation that make up our right to "intellectual privacy."[192] More generally, Professor Daniel Solove has proposed that the First Amendment be recognized as an independent source of criminal procedural protections beyond those afforded by the Fourth Amendment. In particular, he has called for courts to fashion a First Amendment right against intrusive government information-gathering programs that implicate expressive or associational activities and are not narrowly tailored to achieve a substantial government interest.[193]

Taking yet another tack, Matthew Lynch has suggested that, in the surveillance context, a speaker's choice of audience should be considered a form of speech that warrants First Amendment protection from government interference.[194] Even our former-constitutional-law-professor President has conceded the connection between government surveillance and free expression. When asked in December

191 Balkin, *supra* note 122, at 127–30 (warning against government insertion of backdoors into privately owned communication networks).

192 Richards, *supra* note 23, at 1935–36.

193 Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 159–60 (2007).

194 Matthew Lynch, *Closing the Orwellian Loophole: The Present Constitutionality of Big Brother and the Potential for a First Amendment Cure*, 5 FIRST. AMEND. L. REV. 234, 298–300 (2007).

2013 about the NSA surveillance programs, President Obama acknowledged the importance of communications privacy as a component part of "our First Amendment rights and expectations in this country."[195]

The Supreme Court has also recognized that laws protecting conversational privacy advance an important First Amendment interest in facilitating private speech. In *Bartnicki v. Vopper,*[196] the Court held that media outlets that publicly disseminated the contents of an illegally intercepted cell phone call could not be punished under federal or state eavesdropping statutes given that (1) those outlets had not participated in the illegal interception; and (2) the call pertained to a matter of public concern.[197] Although six Justices concluded that the media's First Amendment right to broadcast newsworthy information outweighed the speakers' right to privacy in this instance, all nine Justices recognized the symbiotic relationship between conversational privacy and the willingness of individuals to engage in constitutionally protected speech.[198] Both the majority and the dissent emphasized that actual surveillance need not take place to chill private speech; the mere possibility that one's conversations may be monitored can have a significant speech-inhibiting effect.[199] *Bartnicki* indicates that

195 HARDBALL (NBC television broadcast Dec. 5, 2013) (transcript available at http://www.nbcnews.com/*id*/53755285/ns/msnbc-hardball_with_chris_matthews/t/hardball-chris-matthews-thursday-december-th/#.VIRgfDHF98E).

196 532 U.S. 514 (2001).

197 *Id.* at 534–35.

198 Writing for the majority, Justice Stevens described the case as presenting "a conflict between interests of the highest order—on the one hand, the interest in full and free dissemination of information concerning public issues, and, on the other hand, the interest in individual privacy and, more specifically, in fostering private speech." *Id.* at 518. Justice Breyer, in a concurring opinion joined by Justice O'Connor, described the competing interests at stake as "media freedom" on one side and "personal, speech-related privacy" on the other. *Id.* at 538 (Breyer, J., concurring).

The dissenting Justices, led by Chief Justice Rehnquist, would have given even more weight to the First Amendment rights of cell-phone-using Americans to keep their communications private. The Chief Justice reproached the majority for overemphasizing the First Amendment rights of the media while jeopardizing those of ordinary citizens. *Id.* at 542 (Rehnquist, C.J., dissenting). Noting that, in 2001, approximately 49 million cellular telephones were in use, the Chief Justice concluded that "the chilling effect of the Court's decision upon these private conversations will surely be great." *Id.* at 554 (Rehnquist, C.J., dissenting).

199 The majority and dissent both quoted with approval the following paragraph from the President's Commission on Law Enforcement and Administration of Justice:

> In a democratic society, privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one's speech is being monitored by a stranger, even without the reality of such activity, can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas.

government interference with electronic communications privacy should be open to challenge on First, as well as Fourth, Amendment grounds.

A. The Content/Metadata Distinction and the First Amendment

In *Bartnicki*, the Court recognized the First Amendment value of conversational privacy where the contents of a private phone call had been intercepted and subsequently broadcast by the news media. Bulk metadata collection, conversely, does not involve the capture of communications content; rather, the government vacuums up email and call detail records, collecting the email addresses with which we are in contact, as well as the date, time, duration, and numbers we dial and from which we receive calls. In justifying the NSA's former Section 215 program, the Obama Administration and other supporters relied extensively on the "it's just metadata" argument to assure the American people that it comported with both the First and Fourth Amendments.[200] The one lower court to rule on a First Amendment challenge to the former Section 215 program rejected it, citing Ninth Circuit decisions that upheld under the First and Fourth Amendments the recording by postal workers of envelope information from an individual's incoming mail.[201] Unless the contents of our conversations are seized by the government, this argument goes, any First Amendment right to conversational privacy that may exist has not been compromised.

Well before the advent of electronic databases and computer analytics, Justice Stewart pinpointed the flaw in this argument. Dissenting in *Smith v. Maryland*, he observed that a simple list of numbers dialed by one telephone customer will inevitably disclose substantive information about the content of those calls: it reveals the identities of persons and organizations that the individual attempted to contact.[202] Common sense tells us that Justice Stewart was correct: the

---

Id. at 533; *id.* at 543 (Rehnquist, C.J., dissenting).

200 *See, e.g.*, John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs,* 37 HARV. J.L. & PUB. POL'Y 901, 908 (2014) (stating that "[t]here can be no First Amendment violation if the content of the calls remains untouched"); ADMIN. WHITE PAPER, *supra* note 29, at 21 (emphasizing that the NSA did not collect call content under the former Section 215 program, and arguing that it did not violate the First Amendment).

201 ACLU v. Clapper, 959 F. Supp. 2d 724, 753 (S.D.N.Y. 2013), *rev'd on other grounds,* 785 F.3d 787 (2d Cir. 2015) (citing Lustiger v. United States, 386 F.2d 132, 139 (9th Cir. 1967); Cohen v. United States, 378 F.2d 751, 760 (9th Cir. 1967)).

202 442 U.S. 735, 748 (Stewart, J., dissenting).

gist of a call can often be inferred simply by knowing to whom the call is made. The fact that an individual placed even one call or email to a domestic violence hotline (or a phone sex number) reveals information that the caller may well prefer remain private.[203] Two Stanford researchers demonstrated this obvious conclusion in a 2014 study where they collected three months' worth of metadata from the smartphones of 546 volunteers.[204] Just by looking at isolated numbers dialed by study participants, the researchers were able to surmise intimate details regarding the participants' personal lives:

> Participants had calls with Alcoholics Anonymous, gun stores, NARAL Pro-Choice, labor unions, divorce lawyers, sexually transmitted disease clinics, a Canadian import pharmacy, strip clubs, and much more. This was not a hypothetical parade of horribles. These were simple inferences, about real phone users, that could trivially be made on a large scale.[205]

When the government collects not only the participating phone numbers associated with a call, but the time and duration of those calls (as it does with respect to phone records under EO 12333),[206] the ability to make inferences about conversation content becomes even more pronounced. One need not be an intelligence analyst to glean information from the fact that a person placed a two-hour call to a crisis counseling center at midnight followed by a five-minute call to a psychiatrist's office the next morning. Again, in the Stanford study mentioned above, a mere three months worth of phone metadata allowed researchers to piece together calling patterns that offered revealing glimpses of their subjects' private lives.[207] Given the

---

203 Computer science and public affairs professor Edward W. Felten has observed that with respect to calls to "single-purpose" numbers such as hotlines for rape, domestic violence or addiction, "metadata is often a proxy for content." *Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act, Hearing Before the S. Comm. on the Judiciary*, 113th Cong. 18 (2013) (written testimony of Edward W. Felten, Professor of Computer Sci. & Pub. Affairs, Princeton Univ.), http://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf.

204 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/.

205 *Id.*

206 *See* SPCMA, *supra* note 100, at § 2(a) (defining telephony metadata to include "the telephone number of the calling party, the telephone number of the called party, and the date, time, and duration of the call").

207 Mayer & Mutchler, *supra* note 204. For example, one study participant phoned "multiple local neurology groups, a specialty pharmacy, a rare condition management service, and a hotline for a pharmaceutical used solely to treat relapsing multiple sclerosis." *Id.* Another, within a three-week period, called "a home improvement store, locksmiths, a hydroponics dealer, and a head shop." *Id.* A third subject spoke at length with her sister before making multiple calls to her local Planned Parenthood office. *Id.* These were

revealing nature of these metadata exchanges, the researchers elected not to contact the participants to confirm the substance of their calls. Their conclusion, however, was straightforward: "phone metadata is highly sensitive."[208]

Bulk incidental collection under EO 12333 involves government collection of email and telephony metadata on a much grander scale than the simple pen register information found objectionable by Justice Stewart back in 1979, or the comparatively tiny dataset examined in the Stanford study referenced above. Today's bulk surveillance programs allow the government to collect and store enormous quantities of its citizens' communications metadata in the aggregate and over multiple years for the purpose of subjecting that dataset to high-speed digital analysis.[209] Unsurprisingly, it is actually much cheaper and easier for the government to analyze metadata using advanced computer technology than it would be to have thousands of intelligence agents listening to millions of individual calls.[210] Even the former general counsel of the NSA has admitted that "[m]etadata absolutely tells you everything about somebody's life . . . . If you have enough metadata you don't really need content."[211]

In the context of the former Section 215 program, supporters responded that any fears regarding the revealing nature of metadata were overblown given that the NSA collected only telephone numbers without the corresponding subscriber identities[212]—an argument that could also be applied to incidental bulk collection and analysis under EO 12333. In both instances, however, the conclusion that this

followed by brief calls to Planned Parenthood two weeks later, and one final call to Planned Parenthood at the four-week mark. *Id.*

208 Mayer & Mutchler, *supra* note 204.

209 *See supra* notes 161–63 and accompanying text.

210 *But see* Dan Froomkin, *The Computers are Listening: Speech Recognition is NSA's Best-Kept Open Secret*, INTERCEPT (May 11, 2015), https://theintercept.com/2015/05/11/speech-recognition-nsa-best-kept-secret/ (describing an NSA program that automatically converts spoken content of telephone calls into searchable phonetic transcripts).

211 Alan Rusbridger, *The Snowden Leaks and the Public*, N.Y. REV. OF BOOKS, Nov. 21, 2013 (quoting Stewart Baker), http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/.

212 *See* Jane Mayer, *What's the Matter with Metadata?*, NEW YORKER, June 6, 2013 (describing Senator Diane Feinstein's defense of the former Section 215 program as emphasizing that the NSA collects only phone numbers, not names); *see also* Ryan McDonald, *NSA Director Keith Alexander Defends Data Collection During Baltimore Visit*, BALTIMORE BUS. J., Oct. 31, 2013, http://www.bizjournals.com/baltimore/blog/cyberbizblog/2013/10/nsa-director-keith-alexander-defends.html (reporting that the NSA Director responded to concerns about the former Section 215 program by noting that the agency does not collect caller identities).

renders the metadata anonymous is simply wrong.[213] Most of us have employed publicly available databases to match phone numbers to a name. Given the myriad resources available to the NSA, it must be child's play for such a sophisticated intelligence agency to do the same. If the NSA truly were incapable of determining someone's identity from a phone number, it would be nonsensical for the agency to collect call detail records in the first place. Most email metadata collected under EO 12333, which include the Internet-protocol address of the computer from which an email was sent, as well as log-in information pertaining to web-based email accounts, are also easily identifiable.[214] As an example, consider former CIA Director David Petraeus, who learned this the hard way after the FBI used email metadata to link a pseudonymous email account to his mistress.[215]

All in all, then, communications metadata is powerful stuff. The fact that the government subjects incidentally collected domestic metadata, rather than communications content, to unlimited analysis under EO 12333 should not foreclose further First Amendment scrutiny.

B. Is the Chilling Effect Real?

Given the revealing nature of communications metadata, incidental government collection of domestic email and call records under the guise of foreign collection could pose a threat to our First Amendment freedoms by discouraging citizens from speaking frankly or associating with those whom the government might view with suspicion or disdain. Scholars have argued that government surveillance strips us of the privacy we need to generate new ideas, to test potentially controversial or unpopular views, and to develop our beliefs by sharing them openly with trusted others.[216] Simple awareness that the

213 For a discussion of how easily "anonymized" datasets can be re-identified, see Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1703–04 (2010) (concluding that, because of advances in re-identification science, "[d]ata can be either useful or perfectly anonymous, but never both").

214 *See* SPCMA, *supra* note 100, at § 2(b).

215 *See* Scott Shane & Charlie Savage, *Officials Say F.B.I. Knew of Petraeus Affair in the Summer*, N.Y. TIMES, Nov. 11, 2012, at A1 (detailing the F.B.I.'s use of metadata to ascertain an e-mail author's identity in the investigation of David Patraeus).

216 *See, e.g.*, Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 467 (2015) (concluding that government surveillance discourages the cultivation of minority viewpoints and limits individual autonomy); Richards, *supra* note 23, at 1935 (stating that government surveillance of intellectual activity, such as communicating with others about political and social issues, can discourage experimentation with "new, controversial, or deviant ideas").

government collects, stores and analyzes our communications metadata may make us less likely to communicate, or associate, with others freely and without fear.

In general, social science research confirms the logical conclusion that we act differently when we know, or even suspect, that we are being observed.[217] This is the reason why closed-circuit television cameras have been installed in public streets, transit systems and businesses around the world. Film footage from surveillance cameras may assist law enforcement in solving crimes, but the mere presence of cameras also tends to reduce criminal conduct in the first instance.[218] Similarly, some cities have installed cameras at intersections not only to detect but also to deter drivers from running red lights.[219] These examples show how we often conform our behavior in accordance with social norms when we think we are being watched, even when the only "watcher" is a machine.

Apologists for the former Section 215 program claim that when the government gathers our metadata, it is merely collecting information that we already have provided, willingly, to third party service providers.[220] Speakers who really believe that metadata collection constrains their expressive freedom, the argument goes, would have refused to share their metadata with the telephone company or their Internet service provider in the first place. Even overlooking the ut-

---

217 For example, social scientists found that displaying signs with the message "Cycle Thieves, We Are Watching You" at bike racks on a university campus decreased bicycle thefts at those locations by 62% over a twelve-month period. Daniel Nettle, Kenneth Nott & Melissa Bateson, *'Cycle Thieves, We Are Watching You': Impact of a Simple Signage Intervention Against Bicycle Theft*, PLOS ONE (Dec. 12, 2012), http://journals.plos.org/plosone/article?*id*=10.1371/journal.pone.0051738; *see also* Kaminski & Witnov, *supra* note 216, at 489–93 (listing and describing additional surveillance-related studies).

218 *See, e.g.*, NANCY G. LA VIGNE ET AL., URBAN INST. JUSTICE POL'Y CTR., EVALUATING THE USE OF PUBLIC SURVEILLANCE CAMERAS FOR CRIME CONTROL AND PREVENTION, 87 (2011), http://www.urban.org/sites/default/files/alfresco/publication-pdfs/412403-Evaluating-the-Use-of-Public-Surveillance-Cameras-for-Crime-Control-and-Prevention.PDF (concluding that surveillance cameras, when actively monitored and properly placed, can reduce crime).

219 Based on figures comparing the number of collisions in Seattle during the three years before and after the city installed red-light cameras, the Seattle Department of Transportation found that collisions decreased by about 23% , and collisions involving pedestrians declined by almost one-third. Will Green, *Seattle's Red Light Cameras Reduce Collisions by 23%*, URBANIST (Jan. 23, 2015), http://www.theurbanist.org/2015/01/23/a-look-at-seattles-red-light-cameras/.

220 For instance, at a 2013 debate sponsored by Intelligence Squared U.S., ex-NSA general counsel Stewart Baker described the former Section 215 program not as "spying on everybody," but rather as "gathering data that is already in the hands of third parties." Intelligence Squared U.S., *Spy On Me, I'd Rather Be Safe*, (Nov. 20, 2013), 12–13, http://www.scribd.com/doc/200404032/Spy-on-Me-I-d-Rather-Be-Safe-Transcript.

ter impossibility of surviving in today's world without communications devices that, of necessity, create metadata,[221] this contention assumes that sharing data with a business is no different from providing it to the government, with its singular power to prosecute, investigate and punish.[222] In her *United States v. Jones* concurrence, Justice Sotomayor charged that "[a]wareness that the *Government* may be watching chills associational and expressive freedoms."[223] The President's Review Group quoted Justice Sotomayor to explain its recommendation that Congress terminate the former Section 215 program, adding that public trust in government is seriously weakened when citizens know that the government can access their communications metadata with "one flick of a switch."[224]

Neither Justice Sotomayor nor the President's Review Group, however, cited any empirical support for the conclusion that government surveillance deters speech or association. This is understandable; scholars have often noted the difficulties associated with demonstrating the existence of a chilling effect.[225] Nevertheless, since the Snowden revelations in 2013, various surveys have suggested that Americans are extremely concerned about government surveillance, which has caused us to doubt our ability to communicate privately, and had at least some effect on our communications behavior. According to a 2014 Pew Research Center study, almost 80% of those surveyed agreed or strongly agreed that "Americans should be concerned about the government's monitoring of phone calls and internet communications."[226] More importantly, the study found that most of those surveyed had lost confidence in the privacy of their electron-

221 Back in 2010, the Court recognized the growing importance of cell phones, stating in City of Ontario v. Quon that "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." 560 U.S. 746, 760 (2010).

222 *See* Anjali S. Dalal, *Shadow Administrative Constitutionalism and the Creation of Surveillance Culture*, 2014 MICH. ST. L. REV. 59, 112 (explaining that sharing information with the government is a "different proposition all together [sic]" than sharing that same information with a private company).

223 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (emphasis added). *See also supra* notes 172–75 and accompanying text.

224 PRG Report, *supra* note 85, at 117.

225 *See, e.g.*, Leslie Kendrick, *Speech, Intent, and the Chilling Effect*, 54 WM. & MARY L. REV. 1633, 1675 (2013) (noting that "[i]t is difficult to establish either the presence or absence of a chilling effect, let alone to measure the extent of such an effect"); Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the Chilling Effect*, 58 BOSTON U. L. REV. 685, 730 (1978) (stating that as specific predictions about human behavior, chilling effects are probably "unprovable").

226 Pew 2014 Study, *supra* note 1, at 22.

ic conversations, whether made via landline phones, cell phones, text messaging, instant messaging, email, or social media messaging.[227]

Other studies have focused on the chilling effect of surveillance on writers and members of the press. Journalists depend on the telephone and digital devices to gather newsworthy information, sometimes from sources who insist on remaining nameless. Those sources may be unwilling to communicate by phone or email if they believe that any promise of confidentiality is rendered meaningless by the government's ability to collect and scrutinize their communications metadata.[228] A 2013 PEN America survey of 528 writers/editors found that 76% of respondents believe that government surveillance programs invade the privacy they needed to be creative; as a result, 24% of respondents reported avoiding certain topics when communicating by telephone or email, and 16% said they had limited the topics upon which they wrote or spoke for fear that the government was monitoring their communications.[229] A smaller 2014 ACLU/Human Rights Watch study of U.S. journalists who cover national security issues detailed how the combination of NSA surveillance plus the increased number of prosecutions against government leakers has dried up sources and made information-gathering much more diffi-

227 *Id.* at 23. Unsurprisingly, the more survey respondents knew about government surveillance programs, the less confident they were in their ability to communicate personal information in a confidential manner. *Id.*

A follow-up Pew survey in 2015 reported that of the 87% of adults who were familiar with bulk surveillance programs, 34% (30% of all adults) had "taken at least one step to hide or shield their information from the government." Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RESEARCH CTR., Mar. 16, 2015, at 3. Within that group, 14% said they had spoken more in person rather than communicating over the telephone or online; 13% reported avoiding using certain terms when communicating online; and 11% had not used terms they thought might attract government attention when using internet search engines. *Id.* at 19.

228 Justice Stewart recognized that confidentiality is essential to newsgathering in his dissent in *Branzburg v. Hayes*, where he wrote that "when neither the reporter nor his source can rely on the shield of confidentiality against unrestrained use of [governmental] power, valuable information will not be published and the public dialogue will inevitably be impoverished." 408 U.S. 665, 736 (1972) (Stewart, J., dissenting). *See also infra* notes 314–17 and accompanying text; Ross Coulthart, *Metadata Access is Putting Whistleblowers, Journalists and Democracy at Risk*, BRISBANE TIMES (May 4, 2015), http://www.brisbanetimes.com.au/comment/metadata-access-is-putting-whistleblowers-journalists-and-democracy-at-risk-20150504-1mzfi0.html (describing how an Australian official obtained a journalist's private phone records, to demonstrate how easily those records revealed the identity of the journalist's confidential sources).

229 PEN American Ctr., *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor* (Nov. 12, 2013), https://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.

cult.[230] Participating journalists indicated that government surveillance "constrains their ability to investigate and report on matters of public concern, and ultimately undermines democratic processes by hindering open, informed debate."[231]

In its report on the former Section 215 program, the Privacy and Civil Liberties Oversight Board ("PCLOB")[232] concluded that government collection of telephony metadata created a chilling effect that not only weakens our free press but also discourages citizen participation in political, religious and other organizations.[233] As proof, the PCLOB described how groups ranging from Greenpeace to the National Rifle Association supported legal challenges to the program on the grounds that metadata collection has prevented them from communicating freely with members, contributors, politicians, and others.[234] In one such lawsuit, twenty-two diverse advocacy organizations filed affidavits detailing how, after the Snowden revelations, they experienced a drop in telephone communications from members, whistleblowers, clients, and others.[235] Empirical studies of other instances of government surveillance have demonstrated that it can change behavior in ways that diminish the effectiveness of religious or political organizations and social movements.[236]

---

230 Am. Civil Liberties Union & Human Rights Watch, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy* 22, 24–26 (July 28, 2014), https://www.aclu.org/report/liberty-monitor-all-how-large-scale-us-surveillance-harming-journalism-law-and-american.

231 *Id.* at 24.

232 The PCLOB is an independent, bipartisan executive branch agency that was authorized, as currently structured, by Congress in 2007. *See About the Board*, PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., https://www.pclob.gov/index.html (last visited Sept. 25, 2015) (providing a broad overview of the PCLOB's authority, responsibilities, and history). Its mission is "to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties." PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., https://www.pclob.gov/about-us.html (last visited Sept. 25, 2015). For a discussion of the board's troubled history and how its lack of staffing could limit its overall effectiveness, see Dalal, *supra* note 222, at 121–23.

233 PCLOB Section 215 Report, *supra* note 7, at 162.

234 *Id.* at 164.

235 The affidavits in the lawsuit, First Unitarian Church of Los Angeles v. NSA, Civ. No. 13-3287 (N.D. Cal.) (complaint filed July 16, 2013) are available at https://www.eff.org/document/all-plaintiffs-declarations.

236 *See, e.g.*, Tom Tyler, Stephen Schulhofer & Aziz Z. Huq, *Legitimacy and Deterrence Effects in Counterterrorism Policing: A Study of Muslim Americans*, 44 LAW & SOC'Y REV., 365, 396 (2010) (finding that 20% of surveyed Muslim-Americans reported lower mosque attendance in response to increased law enforcement scrutiny of Muslims).

Another study of seventy-one social justice organizations found that government surveillance caused them to engage in self-censorship, and deprived them of members, donations, and access to space in which to share ideas. Amory Starr, et al., *The Impacts of*

While these polls, studies, and reports provide support for the existence of a chilling effect attached to government collection of communications metadata, some might fault the evidence for being overly anecdotal and conclusory, or for taking inadequate account of multiple causes for behavioral changes. Skeptics might point out that during the year following the Snowden revelations, Americans may not have trusted their cell phones, but they certainly continued to use them.[237]

More importantly, all the studies mentioned in this Part were conducted before Congress passed the Freedom Act, which, as described in Part I, imposed some limits on the NSA's surveillance activities under FISA but had no effect on similar activities under EO 12333. The fanfare accompanying the Freedom Act's passage may well have convinced some Americans that their communications records would no longer reside in NSA databases. Consider as well that NSA intelligence gathering under EO 12333 is veiled in secrecy, making it a safe bet that most Americans know little about how the NSA captures and analyzes American metadata as part of its foreign intelligence mandate. While the Snowden leaks forced the government to admit that the NSA collected almost all of our domestic call detail records under the former Section 215 program, the government has remained silent about the scope of incidental collection of American communications metadata under EO 12333.[238] A government surveillance program regarding which most Americans remain entirely ignorant—despite efforts by NSA whistleblower John Napier Tye to educate the public described in Part I[239]—seems unlikely to exert a major chilling effect on protected speech.

Studies to date, then, establish that revelations about government surveillance programs in general have created anxiety among many Americans regarding the privacy of their communications. Fear regarding this lack of privacy can hinder the operation of our free press, undermine our trust in government, and cause us to second-guess what we say and with whom we associate. Nevertheless, it may be impossible to demonstrate, and implausible to believe, that NSA

State Surveillance on Political Assembly and Association: A Socio-Legal Analysis, 31 QUALITATIVE SOC. 251, 267–68 (2008).

237 In the last quarter of 2014, the nation's four largest wireless communications service providers gained between almost a million to two million new subscribers. *See* Dennis Bournique, *Fourth Quarter 2014 Prepaid Mobile Subscriber Numbers By Operator*, PREPAID PHONE NEWS (Feb. 19, 2015), http://www.prepaidphonenews.com/2015/02/fouth-quarter-2014-prepaid-mobile.html.

238 *See infra* notes 401–05 and accompanying text.

239 *See supra* notes 112–13 and accompanying text.

collection and analysis of American communications metadata under EO 12333 in particular has any untoward effect on First Amendment activities, given that most Americans are unaware of EO 12333's existence. While the Supreme Court has, on occasion, invalidated laws in part based on their purported chilling effects without much in the way of evidence to back up its assumptions,[240] whether the Court would be willing to engage in imaginative speculation in this instance would be, at best, a long shot.

C. If a Chilling Effect Exists, Is It Legally Cognizable under the First Amendment?

Even assuming that government surveillance under EO 12333 results in a discernible chilling effect on citizens' First Amendment activities, the mere existence of a chilling effect on speech or association, by itself, will be insufficient to support a First Amendment claim.[241] Much of government regulation is meant to deter citizens from engaging in certain proscribable acts by imposing criminal punishments or civil liability. This natural and expected result is not constitutionally problematic; it constitutes what Frederick Schauer has described as a "benign chilling effect—an effect caused by the intentional regulation of speech or activity properly subject to government control."[242] The fear of being issued a traffic ticket helps ensure that I obey the speed limit. In the speech context, the threat of civil liability under state libel law is meant to discourage the press from knowingly or recklessly publishing defamatory falsehoods about local officials. In this context, libel law restricts a newspaper's ability to publish speech it knows or should know is false, but properly so; defamatory speech in these circumstances can be punished under existing First Amendment doctrine.[243]

A chilling effect becomes constitutionally suspect, or, in Professor Schauer's lexicon, "invidious," when otherwise proper government

240 *See, e.g.*, Gertz v. Robert Welch, Inc., 418 U.S. 323, 390 (1974) (White, J., dissenting) (arguing that the Court had provided no evidence to conclude that the threat of libel suits brought by private citizens would deter truthful news coverage); Kendrick, *supra* note 225, at 1656–57 (stating that "[i]n signal areas such as defamation and obscenity, the Court has provided no evidence whatsoever to support either its diagnosis of chilling or its favored cure," and citing cases).

241 *See* Younger v. Harris, 401 U.S. 37, 50 (1971) ("[T]he existence of a 'chilling effect,' even in the area of First Amendment rights, has never been considered a sufficient basis, in and of itself, for prohibiting state action.").

242 Schauer, *supra* note 225, at 690.

243 *See, e.g.*, United States v. Stevens, 559 U.S. 460, 468 (2010) (listing defamation as a category of speech that can be regulated under the First Amendment).

regulation has the indirect consequence of discouraging expression that falls within the zone of First Amendment protection because the speaker fears punishment or other adverse consequence.[244] Given the unavoidable uncertainties and costs of both litigation and legal compliance, a would-be speaker may choose to remain silent rather than expose herself to potential criminal prosecution,[245] civil liability,[246] increased costs,[247] retaliation,[248] or loss of a government benefit.[249] For example, the same libel laws that serve to protect individual reputations may also cause risk-averse publishers to err on the side of caution, with the result that truthful matters of public importance remain unexpressed. The Court's landmark decision of *New York Times v. Sullivan*[250] reflects a policy determination that a democratic society is better served by legal rules that encourage free debate even at the cost of overprotecting some defamatory falsehoods.[251]

Even with respect to invidious chilling effects, however, not every law or government activity that somehow discourages constitutionally protected speech will be found to violate the First Amendment. In cases where laws or regulatory programs have been invalidated because they have a chilling effect on speech, those laws have imposed some type of punishment, sanction or threat of reprisal on the speaker. The government must have done something that could harm an individual because of her protected speech.[252] So, for example, in *Sullivan*, the state libel law chilled expression by subjecting speakers

244 Schauer, *supra* note 225, at 693.

245 *See, e.g.*, Smith v. California, 361 U.S. 147, 152–54 (1959) (invalidating a city ordinance that made booksellers criminally liable for unknowing possession of obscene materials).

246 *See, e.g.*, New York Times v. Sullivan, 376 U.S. 254, 277 (1964) (finding that the fear of civil damage awards "may be markedly more inhibiting than the fear of prosecution under a criminal statute").

247 *See, e.g.*, Miami Herald v. Tornillo, 418 U.S. 241, 256–57 (1974) (invalidating a statute that required newspaper editors to provide political candidates with space to respond to published criticisms).

248 *See, e.g.*, Dombrowski v. Pfister, 380 U.S. 479, 486–89 (1965) (finding that repeated labeling by state officials of an organization as "subversive," plus state seizures of the groups' records, scared off potential members and contributors).

249 *See, e.g.*, Speiser v. Randall, 357 U.S. 513, 518–19 (1958) (invalidating a state law that denied property tax exemption to veterans who refused to sign a loyalty oath, stating that "to deny an exemption to claimants who engage in certain forms of speech is in effect to penalize them for such speech").

250 376 U.S. at 279–80 (1964) (holding that to prevail in a libel action, public officials must prove that false statements regarding their official conduct were published with either knowledge of falsity or reckless disregard for the truth).

251 *Id.* at 271–72.

252 In the Court's words, government actions create an unconstitutional chilling effect only when those actions are "regulatory, proscriptive, or compulsory in nature." Laird v. Tatum, 408 U.S. 1, 11 (1972).

to the risk of civil liability. Similarly, in *Miami Herald v. Tornillo*, a state right of reply statute was found to violate the First Amendment because it forced newspapers to pay the costs, in space, paper, and ink, of printing a response to previously published political commentary.[253] Rather than subsidize someone else's speech, the Court concluded, some editors would simply refuse to publish controversial political opinions altogether.[254] The actionable chilling effect resulted from an unconstitutional ultimatum: any editor who chose to express a political opinion could be required to finance someone else's point of view.

Conversely, valid government rules and regulations of general applicability frequently operate to chill even our protected speech in a way that courts view as merely incidental. For example, the presence of airport security may keep me from making jokes about terrorism at the airport, yet we would all agree that the screeners' presence is not constitutionally problematic. In these cases, courts balance the importance of the state interest advanced by the law or regulatory program against the magnitude of the chilling effect on expressive activities.[255] The Court's decision in *Branzburg v Hayes*,[256] a case involving the general duty of all citizens to testify regarding their knowledge of criminal activities, is a good example of this approach. There, the Court refused to grant reporters a special First Amendment right to refuse to testify before grand juries regarding information provided to them by confidential sources, finding that any deterrent effect on the willingness of sources to speak with the press was both uncertain and outweighed by government's countervailing interest in protecting public safety.[257] Only if it could be shown that the government convened a grand jury in bad faith to harass or intimidate a particular journalist, rather than to fight crime, did the Court indicate that the First Amendment would require a different result.[258]

Applying these principles to secret government surveillance programs demonstrates why a stand-alone First Amendment claim based on chilling effects is unlikely to succeed. When the NSA passively col-

253 418 U.S. 241, 256–57 (1974).

254 *Id.* at 257.

255 *See, e.g.*, Younger v. Harris, 401 U.S. 37, 51 (1971) ("Where a statute does not directly abridge free speech, but—while regulating a subject within the State's power—tends to have the incidental effect of inhibiting First Amendment rights, it is well settled that the statute can be upheld if the effect on speech is minor in relation to the need for control of the conduct and the lack of alternative means for doing so.").

256 408 U.S. 665 (1972).

257 *Id.* at 690–91.

258 *Id.* at 707–08.

lects communications metadata under EO 12333, the agency neither prohibits any speech nor imposes any punishment on those who engage in lawful communications. Absent abuse, metadata collection carries no consequence other than the possibility of further investigation should analysis reveal that a U.S. person is in contact with a suspected terrorist. Like *Branzburg*'s requirement that every citizen provide his or her testimony in a criminal case, then, the NSA's bulk collection of communications metadata under EO 12333 is a program of general applicability,[259] and the program's effect on speech will be deemed incidental.[260] The balance of interests cannot help but favor the government, given that foreign-intelligence-gathering activities serve to keep the nation safe from foreign terrorism, a state interest of the highest order.[261] This fundamental state interest cannot be outweighed given that—thanks in large part to government secrecy surrounding the program—the amount of speech chilled by the existence of EO 12333 collection is uncertain at best, and, most likely, insignificant.

A First Amendment challenge to government surveillance based on its chilling effect on freedom of association would seem to provide a stronger basis to oppose NSA surveillance under EO 12333. After all, the whole purpose of collecting communications metadata and subjecting it to potentially unlimited contact chaining under SPCMA[262] is to give the NSA the ability to map social connections among correspondents so it can look for potential terrorists and their collaborators.[263] More than fifty years ago, the Court in *NAACP v. Alabama* held that the state could not force the NAACP to comply with a disclosure order to provide its membership list to state officials, because to do so would violate NAACP members' right to associate to advance their opinions and beliefs.[264] Compelled identification of

259 As described in Part I, EO 12333 collection falls outside of the FISA warrant requirements for the very reason that the NSA does not target specific Americans when it engages in vacuum-cleaner-style foreign-based surveillance. *See supra* Part I. By the same token, untargeted collection of communications metadata would, by definition, fall outside the bad faith exception identified in *Branzburg*. 408 U.S. 665, 707–08 (1972).

260 *See* Wayte v. United States, 470 U.S. 598, 611–13 (1985) (finding that government policy of prosecuting those draft resisters who self-reported their failure to register imposed an incidental burden on speech that was justified by the important interest in effective enforcement of the draft laws).

261 *See, e.g.*, Haig v. Agee, 453 U.S. 280, 307 (1981) ("It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation.").

262 *See supra* notes 94–104 and accompanying text.

263 *See* Strandburg, *supra* note 24, at 327–28 (describing the goal of comprehensive metadata collection as "relational surveillance").

264 357 U.S. 449, 466 (1958).

group members, while not directly stifling speech, could thwart an organization's ability to attract and retain members, especially when a group promotes controversial or unpopular views.[265]

While the Court noted that the right to privacy of group association is not absolute, it concluded that the disclosure order in these facts amounted to a "substantial restraint" on group members' freedom of association.[266] This was so, the Court emphasized, because the NAACP had produced strong evidence that, in the past, its members had been subjected to threats of "economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility."[267] On the other side of the balance, the Court found that the state had failed to demonstrate that disclosure of the membership list substantially advanced its asserted state interest in determining whether the NAACP had complied with Alabama's foreign corporation registration statute.[268]

One obvious difference between *NAACP* and NSA collection of communications metadata is that the NSA compels no organization to reveal its adherents; rather, the NSA has itself gathered the communications metadata from which it infers a target's social connections. In that sense, the government's collection and analysis of metadata could be characterized as an independent investigation, similar to what in the old days would have required the FBI to send a bevy of agents to follow suspected terrorists and monitor their interactions with others. Viewed this way, the government could avoid *NCAAP*'s holding by taking advantage of technological advances that allow it to compile membership lists without having to ask for them. Whether this should make a constitutional difference is doubtful. As Professor Katherine Strandburg has observed with respect to the former Section 215 program, "[t]he fact that associational information must be inferred from the metadata rather than merely read from a list does little to limit the program's potential to chill associational activity."[269]

A more significant distinction is the fact that the chilling effect on association recognized by the Court in *NAACP* resulted from the very real likelihood of reprisals against group members should their iden-

265 *Id.* at 462.
266 *Id.*
267 *Id.*
268 *Id.* at 464–65.
269 Strandburg, *supra* note 24, at 359.

tities be revealed.[270] Not only did the disclosure order target the NCAAP directly, the organization had shown past instances where members, once identified as such, lost their jobs, were physically threatened, and suffered other economic and social harms.[271] In later cases, the Court has required those resisting disclosure requirements on the grounds of associational privacy to show "a reasonable probability that the compelled disclosure . . . will subject them to threats, harassment, or reprisals from either Government officials or private parties."[272] In *Doe v. Reed*, for example, the Court rejected a facial challenge to a state public records act provision that required state officials to provide on request copies of referendum petitions containing the signers' names and addresses.[273] Although the petition signers alleged that disclosure would expose them to harassment and intimidation by groups with opposing political views, the Court found that the signers had provided insufficient evidence to support their fears.[274]

Based on our admittedly limited knowledge, NSA collection of communications metadata under EO 12333 targets no U.S. persons, imposes no punishments, and inflicts no tangible harms (except, perhaps, on terrorists and their associates). While those few Americans who are aware of NSA surveillance under EO 12333 may be less likely to communicate with foreigners or join dissident organizations, this hardly equals the campaign of harassment suffered by NAACP members in Alabama during the 1950s. As a result, courts are unlikely to view the NSA's passive collection of metadata as creating a "serious burden"[275] on Americans' right of expressive association.

Finally, while the Court has indicated that restrictions on freedom of association must survive "exacting scrutiny," those restrictions will be upheld if they "serve compelling state interests, unrelated to the suppression of ideas, that cannot be achieved through means signifi-

270 For a discussion of how the Alabama Citizens' Councils retaliated against civil rights advocates in the 1950s, see John D. Inazu, *The Strange Origins of the Constitutional Right of Association*, 77 TENN. L. REV. 485, 508–10 (2010).

271 *NAACP*, 357 U.S. at 462.

272 Buckley v. Valeo, 424 U.S. 1, 74 (1976) (per curiam); *see also* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 370 (2010) (citing McConnell v. Fed. Election Comm'n, 540 U.S. 93, 198 (2003)).

273 561 U.S. 186 (2010).

274 *Id.* at 199–201. However, the Court acknowledged the possibility of a future as-applied challenge to the law with respect to a particular petition. *Id.* at 201.

275 *See* Boy Scouts of Am. v. Dale, 530 U.S. 640, 658–59 (2000) (noting that "in the associational freedom cases . . . after finding a compelling state interest, the Court went on to examine whether or not the application of the state law would impose any 'serious burden' on the organization's rights of expressive association").

cantly less restrictive of associational freedoms."[276] Foreign intelligence gathering, including NSA collection and analysis of communications metadata, is defended by the government as a means to combat terrorism, an interest described by the Court as "an urgent objective of the highest order."[277] Could the government fight terrorism as effectively without subjecting our communications metadata to indiscriminate collection and analysis? Given the secrecy surrounding EO 12333, it would be impossible for someone without a high-level security clearance to tell. It's worth noting, however, that the Court has recently resolved other questions of free speech and association in the national security context by according great deference to government claims of necessity,[278] a trend that is likely to continue.[279]

D. The Problem of Standing

All of this discussion may be academic in the sense that it overlooks a more fundamental problem: even if government collection and analysis of domestic communications metadata chills speech and/or association, will anyone have standing to seek redress in court? Under Article III standing doctrine, to have a justiciable claim, a litigant must demonstrate that she has suffered an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[280] In the surveillance context, the Supreme Court has interpreted the first two of these requirements to make it next to impossible for litigants to mount a court challenge to secret government surveillance programs.

The Court first addressed a challenge to government surveillance in *Laird v. Tatum*,[281] where the plaintiffs objected that their First Amendment rights had been chilled by the "mere existence" of a U.S.

---

276 Roberts v. U.S. Jaycees, 468 U.S. 609, 623 (1984). So, for example, the Court has upheld federal campaign finance disclosure requirements despite their potential chilling effect on would-be donors based on the compelling state interest in informing the electorate and countering campaign corruption. *Buckley*, 424 U.S. at 68.

277 Holder v. Humanitarian Law Project, 561 U.S. 1, 28 (2010).

278 *Id.* at 7 (upholding federal law prohibiting provision of "material support or resources" to certain terrorist organizations against free speech and free association claims brought by human rights organizations).

279 *See* Dalal, *supra* note 222, at 114–16 (describing how courts grant the executive branch a type of "super-deference" with respect to national security matters).

280 Monsanto Co. v. Geerston Seed Farms, 561 U.S. 139, 149 (2010) (citing Horne v. Flores, 557 U.S. 433, 445 (2009)).

281 408 U.S. 1 (1972).

Army program that compiled information regarding lawful civilian political activities thought to present a risk of civil disorder.[282] A 5-4 majority dismissed the plaintiffs' claim as non-justiciable, holding that "allegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm."[283] While the Court in *Laird* did not reach the merits of the First Amendment claim, it emphasized that the plaintiffs had presented no evidence that the government had engaged in any illegal surveillance practices; in fact, most of the information collected by Army intelligence agents came from public sources such as the news media.[284] The Court indicated that its decision might have been different had the government engaged in unlawful conduct, stating that nothing in its holding "can properly be seen as giving any indication that actual or threatened injury by reasons of unlawful activities of the military would go unnoticed or unremedied."[285]

More than forty years later, however, plaintiffs who claimed that a secret government surveillance program was unlawful under the First and Fourth Amendments, Article III and separation of powers doctrine fared no better. In *Clapper v. Amnesty International USA*,[286] the Court extended the *Laird* holding to deny standing to plaintiffs who alleged to have suffered both actual and threatened harm from covert government surveillance conducted under Section 702 of FISA.[287] That program authorizes the NSA to capture communications of non-U.S. persons who are reasonably believed to be located outside the United States without a showing of individualized suspicion.[288] However, Section 702 also expands the government's ability to monitor Americans' communications, given that U.S. persons who communicate with foreigners may also have their private messages "incidentally" collected.[289]

The *Clapper* plaintiffs consisted of U.S. persons whose work as attorneys, human rights activists, and journalists required them to

282 *Id.* at 2, 10.
283 *Id.* at 12–14.
284 *Id.* at 9.
285 *Id.* at 16.
286 133 S. Ct. 1138 (2013).
287 *Id.* at 1143.
288 50 U.S.C. § 1881a(a)–(b) (2012) (allowing the AG and the DNI to jointly authorize, for the purpose of acquiring foreign intelligence information, the surveillance of non-U.S. persons who are reasonably believed to be located abroad).
289 For more information about the Section 702 program, including incidental collection of communications belonging to or concerning U.S. persons, see the PCLOB Section 702 Report, *supra* note 93.

communicate by telephone and email with foreigners who were likely targets of Section 702 surveillance.[290] The plaintiffs argued that, as a result of their reasonable fear that their overseas electronic communications would be intercepted by the NSA, their future ability to gather information, develop sources, and communicate privately with their clients would be impaired.[291] Additionally, they claimed that the surveillance threat had already forced them to take "costly and burdensome measures," such overseas travel, to ensure the confidentiality of their conversations.[292]

In a 5-4 decision, the Court rejected these arguments. First, the plaintiffs' claims of likely future injury were seen by the Court as too speculative because the plaintiffs had failed to establish that their communications had been or would be, in fact, intercepted by the government.[293] (Of course, plaintiffs had no way to prove this—secrecy is, by definition, an essential component of covert government surveillance.) What the plaintiffs, and the Court of Appeals, saw as an "objectively reasonable likelihood"[294] that the plaintiffs' communications would be monitored was, to the Court, nothing more than a "speculative chain of possibilities" insufficient to demonstrate the existence of a "certainly impending" injury.[295]

Compounding the plaintiffs' problems with proof was the fact that the government has multiple legal authorities under which it can conduct foreign surveillance, including EO 12333. For plaintiffs to survive the traceability prong of the standing test, Justice Alito reasoned that plaintiffs would have to demonstrate not only that their communications actually had been intercepted by the NSA, but also that the interceptions occurred pursuant to Section 702 and not some other statutory provision or executive order.[296] Even in the rare case where a plaintiff could produce actual evidence of covert government surveillance, the existence of overlapping legal authorities for intelligence gathering means that a plaintiff may never be able to demonstrate conclusively that she was surveilled pursuant to one authority or another.

---

290 For example, two plaintiffs were attorneys who had represented Guantanamo Bay detainees charged with terrorism. *Clapper*, 133 S. Ct. at 1157–58 (Breyer, J., dissenting).

291 *Id.*

292 *Id.* at 1146.

293 *Id.* at 1148.

294 *Id.* at 1143, 1146 (citing Amnesty Int'l United States v. Clapper, 638 F.3d 118, 133, 134, 139 (2d Cir. 2011)).

295 *Id.* at 1150.

296 *Id.* at 1149.

Second, Justice Alito also rejected the plaintiffs' argument that they had already suffered a sufficient injury for standing purposes given the expenses they had incurred to ensure the privacy of their communications. According to the Court, any economic costs borne by the plaintiffs could not fairly be attributed to Section 702 surveillance, but rather were the product of plaintiffs' own subjective, hypothetical—but admittedly not irrational—fears.[297] Justice Alito expressed concern that a contrary decision would allow the plaintiffs to "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[298] He was apparently less concerned that the Court's reasoning allowed the government to defeat standing simply by keeping silent and insisted that the Court's holding would not insulate Section 702 from judicial review. Because FISA requires that the government provide notice of its intent to use information derived from Section 702 in a criminal prosecution, Justice Alito noted that defendants who receive such notice could bring a constitutional challenge to the statute.[299]

Writing for the dissenters, Justice Breyer disputed the Court's finding that the plaintiffs' future injuries were too speculative, noting that Section 702 surveillance of plaintiffs' communications in these facts was "as likely to take place as are most future events that com-

297 *Id.* at 1151 (stating that "[i]f the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear").

298 *Id.*

299 Under FISA, the government is required to notify defendants when it uses evidence "obtained or derived" from Section 702 surveillance. 50 U.S.C. §§ 1806(c), 1881e(a). Ironically, at the time *Clapper* was argued and decided, the Department of Justice was not providing this required notice to criminal defendants, in direct contradiction of assurances given to the Court by the Solicitor General. *See* Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. TIMES, July 16, 2013, at A11 (explaining that despite the solicitor general's assertions, federal prosecutors refused to make the requisite disclosures in criminal prosecutions). Since that time the government has notified at least two criminal defendants that evidence had been obtained against them pursuant to warrantless surveillance under the Section 702 program. *See* Ellen Nakashima, *Man Convicted in Terrorism Case Seeks Evidence from Warrantless NSA Surveillance*, WASH. POST, (Jan. 13, 2014), https://www.washingtonpost.com/world/national-security/man-convicted-in-terror-case-challenges-warrantless-spying/2014/01/13/af7da5de-7cba-11e3-95c6-0a7aa80874bc_story.html (noting that federal prosecutors notified a defendant in Colorado as well as a defendant in Oregon "that evidence from a warrantless wiretap was used against [them]"). One of these defendants brought a constitutional challenge to Section 702, which was rejected by a federal district court. *See* United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 U.S. Dist. LEXIS 85452, at *30, *32 (D. Or. June 24, 2014) (rejecting defendant's arguments challenging the constitutionality of Section 702 under the First and Fourth Amendments).

monsense inferences and ordinary knowledge of human nature tell us will happen."[300] This was so, Justice Breyer reasoned, because the government had both strong motives as well as the technical ability to intercept communications belonging to the plaintiffs' foreign contacts.[301] A "reasonable probability" of harm, not an absolute certainty of occurrence, had been required by the Court in past cases and, according to Justice Breyer, was the appropriate standard for the Court to grant standing in these facts.[302]

Commentators were quick to fault *Clapper* for setting the standing barrier so high as to make it virtually impossible to bring a public interest lawsuit to challenge secret government surveillance programs.[303] Legal scholars have criticized the Court's "certainly impending" requirement[304] as well as its cramped conception of "injury," arguing that covert surveillance results in numerous harms both to individuals and to society that should be recognized as such in standing doctrine.[305] And while the Court's decision did not entirely close the courthouse door with respect to the constitutionality of the Section 702 program thanks to FISA's defendant-notification provision,

300 *Clapper*, 133 S. Ct. at 1155 (Breyer, J., dissenting).

301 *Id.* at 1158–59.

302 *Id.* at 1165.

303 *See, e.g.*, Editorial, *Unbridled Secrecy*, N.Y. TIMES, Feb. 27, 2013, at A24 (calling the decision a "clear-cut abdication of its fundamental role in the American constitutional system of checks and balances"); Jonathan Turley, *Supreme Court Rejects Challenge to Secret Surveillance*, RES IPSA LOQUITUR (Feb. 27, 2013), http://jonathanturley.org/2013/02/27/supreme-court-rejects-challenge-to-secret-surveillance/ (describing decision as "a true nightmare for civil liberties").

304 *See, e.g.*, Vicki C. Jackson, *Standing and the Role of Federal Courts: Triple Error Decisions in* Clapper v. Amnesty International USA *and* City of Los Angeles v. Lyons, 23 WM. & MARY BILL OF RTS. J. 127, 144–46 (2014) (suggesting that the Court follow the lead of the European Court of Human Rights to hold that individuals may challenge covert surveillance if they can show a "reasonable likelihood" of having been subject to surveillance or that they are members of a group that is "at risk" of being surveilled); Slobogin, *supra* note 38, at 520 (arguing that "any litigant whose participation in the political process is concretely affected by covert surveillance should have standing" to challenge that surveillance).

305 *See, e.g.*, Jackson, *supra* note 304, at 134–35 (contending that by denying justiciability in *Clapper*, the Court potentially harmed millions of Americans' privacy rights, created an incentive for unlawful leaks of classified information, impaired democratic self-governance, and damaged the Court's role in our constitutional system); Kaminski & Witnov, *supra* note 216, at 514–15 (suggesting that surveillance creates a "conforming effect" that should be considered as an injury for the purposes of standing); Richards, *supra* note 23, at 1936 (arguing that standing doctrine should recognize that surveillance "menaces intellectual privacy and increases the risk of blackmail, coercion, and discrimination"); Slobogin, *supra* note 38, at 519–20 (asserting that covert government surveillance harms the political process).

no comparable notice requirement applies to evidence derived from an EO 12333 intercept.[306]

Unchecked executive branch surveillance power presents serious risks to privacy, speech and our democratic processes. Left unrestrained, the government's exercise of that surveillance power is likely to continue to expand. If the judicial branch is to play its constitutionally mandated role in our political system, persons with non-frivolous claims of objectively reasonable harm stemming from credible constitutional violations should not be barred from seeking judicial redress, especially when the claims relate to a topic as vital to our free society as covert government surveillance. Accordingly, the Court should abandon *Clapper*'s overly narrow conception of standing, and allow putative plaintiffs to pursue their claims as long as they can demonstrate an objectively reasonable likelihood of injury from the chilling effects of government surveillance. However, while *Clapper* remains the controlling precedent, it will impose a near-insurmountable threshold requirement for law-abiding Americans to challenge secret government surveillance programs based on the First or Fourth Amendments.

IV. AT THE CONVERGENCE OF PRIVACY AND SPEECH

So far, this Article has looked at bulk government collection and analysis of domestic communications metadata from two isolated perspectives. Part II showed how, under the Fourth Amendment, the third party doctrine holds that Americans have no reasonable expectation of privacy in the transactional data relating to their communications, including the phone numbers or addresses (physical or email) with which they correspond. With respect to the First Amendment, Part III demonstrated that, under relevant caselaw, government surveillance programs that neither prohibit nor punish speech, nor target the communications of any particular group, are unlikely to present a cognizable, invidious chilling effect on speech or association. As the crowning blow, the Court narrowed the rules of standing in *Clapper v. Amnesty International USA*[307] to make it almost

306 *See* Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, N.Y. TIMES, Aug. 14, 2014, at A12, A14 (citing assertions by government officials that criminal defendants are not entitled to notice if surveillance conducted under EO 12333 leads to evidence used against them).

307 133 S. Ct. 1138, 1150 (2013) (requiring that plaintiffs establish that their "injury based on potential future surveillance is certainly impending or is fairly traceable to [Section 702]"). *See supra* notes 286–306 and accompanying text.

impossible for a First or Fourth Amendment challenge to a covert government surveillance program to be heard in court at all.

Given our much-vaunted constitutional rights of privacy and free expression, how can this be the right result? Putting the standing question to one side, are the protections of the First and Fourth Amendments really so tepid that the government can accidentally-on-purpose gather and scrutinize enormous quantities of our so-called "foreign" communications records in an unlimited fashion and with impunity? Surely the serious risks to privacy, as well as the grave dangers of official abuse, presented when the government accumulates its citizens' communication records for future analysis deserve more searching Fourth Amendment consideration than perfunctory dismissal under the third party doctrine.[308] By the same token, it is beyond dispute that citizens in a democracy need secure, private methods of communication to facilitate both personal and political expression and association, as well as to ensure the proper functioning of both a free press and a representative government. Government collection and analysis of what are essentially domestic communication records, therefore, implicates our rights to self-government, conversational privacy, personal and political association, autonomy and basic liberty—all First Amendment interests that should be recognized in determining the constitutionality of an official surveillance regime[309]—even if those communications traveled through a foreign cable or happen to be stored on an extraterritorial back-up server.

---

308 This constitutional insufficiency has, of course, been observed by others. *See, e.g.*, Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 104 (2008) (arguing that the third party doctrine would allow the government to deploy secret, undercover spies to record all of our public acts and conversations, a "totalitarian form of surveillance deeply antithetical to the freedom from state scrutiny of our personal lives for which the Fourth Amendment stands").

309 Almost fifty years ago, and a generation before the invention of modern surveillance technology, Justice William O. Douglas recognized the First Amendment implications of government surveillance:

> The time may come when no one can be sure whether his words are being recorded for use at some future time; when everyone will fear that his most secret thoughts are no longer his own, but belong to the Government; when the most confidential and intimate conversations are always open to eager, prying ears. When that time comes, privacy, and with it liberty, will be gone. If a man's privacy can be invaded at will, who can say he is free? If his every word is taken down and evaluated, or if he is afraid every word may be, who can say he enjoys freedom of speech? If his every association is known and recorded, if the conversations with his associates are purloined, who can say he enjoys freedom of association? When such conditions obtain, our citizens will be afraid to utter any but the safest and most orthodox thoughts; afraid to associate with any but the most acceptable people. Freedom as the Constitution envisages it will have vanished.

Osborn v. United States, 385 U.S. 323, 353–54 (1966) (Douglas, J., dissenting).

In this Part, I contend that the First Amendment value of communications privacy must be factored into the determination of whether a government surveillance program violates the Fourth Amendment.[310] When considered in tandem this way, the two Amendments mutually reinforce each other and create a synergy that extends the protections of each.[311] This is more than mere constitutional theory; the Supreme Court has taken this exact approach with respect to domestic security surveillance in the landmark 1972 case of *United States v. U.S. District Court* (the *Keith* case).[312] There, the Court incorporated First Amendment values into its Fourth Amendment analysis to hold that electronic surveillance of U.S. citizens who had no relation to foreign terrorism was unreasonable without a warrant. *Keith* provides the appropriate method of analysis/precedent for the Court to reconsider and limit the third party doctrine in the context of bulk government collection of communications metadata. The question then becomes how both Fourth and First Amendment considerations, as well as the undisputedly essential need to keep our nation safe from foreign terrorism, can be accommodated in the implementation of government surveillance programs that incidentally sweep in records of U.S. person communications.

A. "Scrupulous Exactitude"

Both courts and commentators have often noted the strong historical connection between the First and the Fourth Amendments.[313] In the words of Justice William J. Brennan, Jr., "[t]he Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."[314] From its inception, the Fourth Amendment was designed to protect the First Amendment values of free speech

310 Professor Akhil Reed Amar urged this approach to the Fourth Amendment more than twenty years ago, long before the Snowden era of NSA surveillance. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 805 (1994) ("In thinking about the broad command of the Fourth Amendment, we must examine other parts of the Bill of Rights to identify constitutional values that are elements of *constitutional* reasonableness.").

311 *See* Griswold v. Connecticut, 381 U.S. 479, 483 (1965) ("[T]he First Amendment has a penumbra where privacy is protected from governmental intrusion.").

312 407 U.S. 297 (1972).

313 *See, e.g.*, Stanford v. Texas, 379 U.S. 476, 482 (1965) (stating that the history of the Fourth Amendment "is largely a history of conflict between the Crown and the press"); *see also* Solove, *supra* note 193, at 133 ("The First, Fourth, and Fifth Amendments share a common background in concerns about seditious libel.").

314 Marcus v. Search Warrant, 367 U.S. 717, 729 (1961).

and press from government abuse of its investigative powers. That the interplay between privacy and speech should make a difference in the strength of Fourth Amendment protections has been recognized by the Court, starting in a series of cases dealing with government seizures of books and films alleged to be obscene. In these cases, the Court invalidated large-scale seizures of multiple copies of magazines and books, even though authorities had valid search warrants that would have satisfied the Fourth Amendment in another context.[315] Because even obscene publications enjoy presumptive First Amendment protection, the Court found that pretrial seizures of those materials require pre-seizure procedures "designed to focus searchingly on the question of obscenity."[316]

The presence of First Amendment values has also caused the Court to interpret Fourth Amendment warrant exceptions more narrowly. In *Roaden v. Kentucky*,[317] a local sheriff viewed a movie at a drive-in theater, determined that it was obscene, arrested the theater manager in the projection booth for displaying obscenity, and removed one copy of the film as evidence.[318] While the lower court upheld the seizure as incident to a lawful arrest, a standard warrant exception,[319] the Supreme Court reversed, warning that the Fourth Amendment "must not be read in a vacuum."[320] Seizures of weapons or contraband must be differentiated, the Court said, from seizures of books or films, where First Amendment values are also in play. "The setting of the bookstore or the commercial theater, each presumptively under the protection of the First Amendment," Chief Justice Burger wrote for the Court, "invokes such Fourth Amendment warrant requirements because we examine what is 'unreasonable' in the light of the values of freedom of expression."[321] *Roaden* stands for the proposition that Fourth Amendment reasonableness must be redefined pursuant to stricter standards when First Amendment interests are implicated by the search or seizure in question.[322]

315 A Quantity of Books v. Kansas, 378 U.S. 205 (1964); *Marcus*, 367 U.S. at 738.

316 *Marcus*, 367 U.S. at 732; *see also Quantity of Books*, 378 U.S. at 210–11 (quoting *Marcus*, 367 U.S. at 732).

317 413 U.S. 496 (1973).

318 *Id.* at 497–98.

319 *See, e.g.*, Chimel v. California, 395 U.S. 752, 762–63 (1969) (explaining that when an arrest is made, it is reasonable for the arresting officer to search the person of the arrestee for weapons and/or evidence, along with the area "within his immediate control" without a search warrant).

320 *Roaden*, 413 U.S. at 501.

321 *Id.* at 504.

322 *Id.*

Yet in a case that presented a paradigmatic example of a conflict between the state and the press, the Court in *Zurcher v. Stanford Daily*[323] paid mere lip service to its "scrupulous exactitude" formulation to approve an innocent third-party search of a newsroom. In that case, Stanford's student newspaper had published articles and photographs about a student demonstration in which police officers had been hurt. Suspecting that the newspaper's files might contain additional photographs of the melee that would help identify the assailants, police obtained an ex parte warrant and searched the newspaper's offices.[324] Outraged that the police had used a knock-on-the-door search rather than a subpoena *duces tecum* to obtain any relevant photographs (of which there were none), the newspaper and its staff brought a civil rights suit for declaratory and injunctive relief, arguing that the search violated their rights under the First and Fourth Amendment.[325]

After citing the obscenity cases for the idea that "unrestricted power of search and seizure could also be an instrument for stifling liberty of expression,"[326] the Court then failed to heed its own admonition. Here, the fact that this was a newsroom seemed to add nothing to the Court's Fourth Amendment calculus, despite the newspaper's argument that the search would disrupt its operations, threaten its ability to protect confidential sources, and chill its newsgathering activities and editorial deliberations.[327] All of these interests had been adequately protected, according to the Court, by the issuance of a warrant.[328] The Court's approach, in effect, removed all substance from the "scrupulous exactitude" language; it requires courts to do no more than what the Fourth Amendment already obligates them to do in any case involving a search or seizure.

The Court went wrong in *Zurcher* by refusing to apply the analysis it had commanded it *Roaden*; it failed to determine what was reasonable under the Fourth Amendment "in the light of the values of freedom of expression." By placing too much emphasis on the fact that "[i]n the normal course of events, search warrants are more difficult to obtain than subpoenas,[329] the Court assumed that the warrant re-

323 436 U.S. 547 (1978).
324 *Id.* at 550–51.
325 *Id.* at 550–52.
326 *Id.* at 564 (quoting Marcus v. Search Warrant, 367 U.S. 717, 729 (1961)).
327 *Id.* at 563–64.
328 *Id.* at 565.
329 *Id.* at 562–63.

quirement provides the highest level of constitutionally mandated privacy protections in all circumstances.[330] But a newsroom search is not a normal event, and on these facts, a subpoena would have been much more effective at guarding the newspaper's valid First Amendment concerns.[331] In dissent, Justice Stewart catalogued the First Amendment values that the Court had ignored, concluding that newsroom searches were "wholly inimical to the First Amendment."[332] The decision unleashed a torrent of criticism from the press,[333] commentators,[334] legislators[335] and various citizens' groups.[336] As a result, Congress remedied the Court's error two years later by passing the Privacy Protection Act,[337] which prohibits federal, state and local law enforcement from searching newsrooms or seizing journalists' work product materials except in certain limited circumstances.

B. The Keith *Case*

While the Court's misguided approach in *Zurcher* demonstrates how the Fourth Amendment, when applied alone, can be insufficient to protect First Amendment interests, the Court's decision in *United*

330 In the words of Professor Amar, *Zurcher* is an example of the Court in thrall to "Fourth Amendment worship of the warrant." Amar, *supra* note 310, at 805.

331 Had police used a subpoena, a surprise intrusion by law enforcement into a working newsroom, as well as the attendant police inspection of confidential files, would have been avoided. Furthermore, a subpoena can be disputed or modified in court on disclosure grounds before compliance, while a search warrant cannot be challenged until after it has been executed.

332 Zurcher, 436 U.S. at 573 (Stewart, J., dissenting).

333 *See, e.g.*, James Kilpatrick, *High Court and Freedom of the Press*, TOLEDO BLADE, June 9, 1978, at 16, https://news.google.com/newspapers?*id*=fxhPAAAAIBAJ&sjid=bAIEAAAAIBAJ&pg=7002%2C3601292 (describing majority opinion in Zurcher as displaying an "astonishing ignorance of the real-world nature of the news-gathering process"); James Reston, *A Letter to the Whizzer*, N.Y. TIMES, June 2, 1978, at A23 (suggesting that, under *Zurcher*, President Nixon could have seized the Pentagon Papers and thereby prevented publication of stories based on those documents).

334 *See, e.g.*, Charles L. Cantrell, Zurcher*: Third Party Searches and Freedom of the Press*, 62 MARQUETTE L. REV. 35, 36 (1978) (describing the decision as "a very real threat to the freedom of the press").

335 *See, e.g.*, Richard L. Strout, *Press Freedom Vote Sets Stage for Court Reassessment*, CHRISTIAN SCI. MONITOR, Sept. 25, 1980, at 7 (quoting House Rep. Robert W. Kastenmeier that *Zurcher* "swept away 200 years of jurisprudence greatly limiting searches directed against innocent third parties").

336 *See, e.g.*, Birch Bayh, *Police Searches of Innocent Third Parties: A Congressional Response to* Zurcher v. Stanford Daily, 6 J. LEGIS. 7, 8 (1979) (describing broad-based support for Congressional reform in response to *Zurcher* ruling).

337 Pub. L. No. 96-440, 94 Stat. 1879 (1980) (codified at 42 U.S.C. § 2000aa (2012)).

States v. U.S. District Court (the *Keith* case)[338] exemplifies how the two Amendments can and should work together in cases involving the First Amendment values associated with conversational privacy and government surveillance.

The *Keith* case emerged out of the civil unrest of the late 1960s and early 1970s.[339] The story began shortly before midnight on September 29, 1968, when several sticks of dynamite exploded outside a Central Intelligence Agency recruitment office in Ann Arbor, Michigan.[340] Although no one was hurt, the blast blew a hole in the sidewalk, smashed windows and resulted in thousands of dollars of property damage.[341] A similar string of bombings had occurred in Detroit, and within two weeks, another dynamite bomb went off in Ann Arbor, this time at the University of Michigan's Institute of Science and Technology.[342]

About a year later, a federal grand jury indicted three members of the White Panther Party, including Lawrence "Pun" Plamondon, for destruction of government property in connection with the CIA office bombing.[343] Before trial, the defense filed a motion to compel the government to disclose any records of electronic surveillance conducted with respect to the defendants. In response, the government filed an affidavit from Attorney General John Mitchell admitting that Plamondon had been overheard by government agents on a warrantless wiretap employed to collect intelligence regarding "subversive" domestic organizations deemed to be a threat to the national security.[344] The government argued that this surveillance, although conducted without any prior judicial approval, was nevertheless legal pursuant to the President's power to protect national security.[345]

338 407 U.S. 297 313–15 (1972). "Keith" refers to Judge Damon J. Keith, the federal district judge who heard the case.

339 Although the opinion contains scant discussion of the underlying facts, the case presented a fascinating back-story involving a Who's Who of counterculture heroes and villains. For more details regarding the case and its cast of characters, see Samuel C. Damren, *The* Keith *Case*, 11 CT. LEGACY, at 1 (Historical Soc'y for the U.S. Dist. Court for the E. Dist. Mich.) (Nov. 2003), https://members.fbamich.org/Portals/31/Documents/Newsletters/200311_Court_Legacy.pdf; Trevor W. Morrison, *The Story of* United States v. United States District Court *(*Keith*): The Surveillance Power*, *in* PRESIDENTIAL POWER STORIES 287, 288 (Christopher H. Schroeder & Curtis A. Bradley eds., 2009).

340 *See* Christopher Zbrozek, *The Bombing of the A2 CIA Office*, MICH. DAILY (Oct. 24, 2006), http://www.michigandaily.com/content/bombing-a2-cia-office.

341 *Id.*

342 *Id.*

343 Morrison, *supra* note 339, at 291–93. The White Panthers were a radical activist group patterned after the Black Panthers and formed by Plamondon and John Sinclair. *Id.*

344 *Keith*, 407 U.S. at 300.

345 *Id.* at 301.

Judge Keith disagreed, holding that the surveillance violated the Fourth Amendment and ordering the government to disclose the overheard conversations to the defense.[346] The government challenged Judge Keith's order through a writ of mandamus,[347] which made Judge Keith the respondent in the appellate courts.

When the mandamus suit reached the Supreme Court in 1972, it presented an issue that the Court specifically had left unaddressed in *Katz v. United States*: "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security."[348] The Court upheld Judge Keith's order, holding that the government must obtain a warrant before engaging in domestic national security surveillance.[349] Importantly, the Court reached its holding by emphasizing the interplay between the Fourth and First Amendments in surveillance cases, noting that while "the investigative duty of the executive may be stronger in [national security] cases, so also is there greater jeopardy to constitutionally protected speech."[350]

Writing for the Court, Justice Lewis Powell conceded that, at least since the time of the Truman Administration, American Presidents had employed electronic surveillance to protect the nation from both internal and foreign threats.[351] But just because a practice is common, Justice Powell observed, does not make it desirable. While electronic surveillance may at times be necessary to safeguard the public interest, Justice Powell perceived the risk to privacy presented by government surveillance as both unsettling and frightening to law-abiding citizens.[352] To protect that privacy, Justice Powell turned to the Bill of Rights, noting that constitutional protections do not fall by the wayside simply because the government cites national security as its reason for engaging in surveillance. Quite the opposite, in fact—Justice Powell stressed that national security cases "often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime."[353] History teaches that surveillance targets are often chosen because of their unorthodox political beliefs; as a

346 *Id.*
347 *Id.*
348 389 U.S. 347, 358 n.23 (1967). *See supra* notes 132–38 and accompanying text.
349 *Keith*, 407 U.S. at 320.
350 *Id.* at 313.
351 *Id.* at 310–11.
352 *Id.* at 312 ("There is, understandably, a deep-seated uneasiness and apprehension that this [surveillance] capability will be used to intrude upon cherished privacy of law-abiding citizens.").
353 *Id.* at 313.

result, Justice Powell instructed courts to apply Fourth Amendment safeguards with a sharp eye to protecting First Amendment rights:

> 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.[354]

Although the Fourth Amendment's primary purpose was to prevent unauthorized government intrusions into the home, Justice Powell cited *Katz* to emphasize that the Amendment's "broader spirit now shields private speech from unreasonable surveillance."[355] To the *Keith* Court, unreasonable surveillance, at least in the context of domestic security, meant warrantless surveillance.[356] To ensure that the constitutional values associated with conversational privacy are guaranteed, Justice Powell insisted that the government obtain prior judicial authorization before spying on Americans for domestic security purposes.[357] However, given the practical and policy considerations associated with national security surveillance, Justice Powell suggested that Congress could enact special domestic security warrant requirements different from those imposed by the federal wiretap act. "Different standards may be compatible with the Fourth Amendment," he wrote, "if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[358]

Finally, the Court stressed that it was expressing no opinion regarding whether the President could engage in warrantless electronic surveillance with respect to foreign powers or their agents.[359] While the Court admitted that the distinction between domestic and foreign security surveillance might, in other cases, be hard to draw, the government here had presented no evidence that a foreign power had been directly or indirectly implicated in the CIA bombing. Attorney General Mitchell's affidavit established that Plamondon's calls had been overheard on wiretaps employed to gather intelligence re-

---

354 *Id.* at 314.

355 *Id.* at 313.

356 The Court's insistence on a warrant exemplifies what has been described as the "warrant preference model of reasonableness"—a view that the modern Court has moved away from, at least at times, in favor of a balancing approach. Cynthia Lee, *Reasonableness With Teeth: The Future of Fourth Amendment Reasonableness Analysis*, 81 MISS. L.J. 1133, 1135 (2012).

357 *Keith*, 407 U.S. at 318. ("Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights.").

358 *Id.* at 322–23.

359 *Id.* at 308–09, 321–22.

garding threats posed by domestic organizations, a term that the Court defined as "a group or organization (whether formally or informally constituted) composed of citizens of the United States and which has no significant connection with a foreign power, its agents or agencies."[360] While Plamondon may have been involved in a criminal conspiracy, the government had no reason to suspect him of associating or collaborating with foreign terrorists.

Although *Keith* was decided more than 40 years ago, the opinion continues to be the Court's most significant analysis of the constitutional questions pertaining to warrantless electronic surveillance of American citizens. In that regard, *Keith* teaches at least three important lessons that remain relevant today. First, the case reminds us that even when government surveillance is justified to protect valid national interests, it is properly classified as a necessary evil. It must be used cautiously and sparingly, because "even when employed with restraint and under judicial supervision," surveillance creates anxiety and distrust among law-abiding citizens.[361] Secret, warrantless surveillance violates our constitutional norms; the Bill of Rights leads us to expect that, if we haven't done anything wrong, the government will respect our valued right to conversational privacy.

Second, *Keith* establishes that First Amendment interests must be both recognized and accorded real weight in determining whether government surveillance of domestic communications comports with the Fourth Amendment. In a field like national security where First and Fourth Amendment values converge, the *Keith* case tells courts to consider those rights in tandem rather than in isolation. According to Justice Powell, courts must balance the government's duty to protect national security against the potential danger surveillance poses to both "individual privacy and free expression."[362] Imagine a Venn diagram that illustrates overlapping spheres; where First and Fourth Amendment forces unite, the protections of both Amendments reinforce and gain strength from each other.

The third lesson to take from *Keith* is that the distinction between domestic and foreign security is to be determined not only based on the purpose of the surveillance, but also on the characteristics of the individuals or groups being surveilled. Attorney General Mitchell's affidavit established that Plamondon's calls had been overheard on wiretaps employed to gather intelligence regarding threats posed by

360 *Id.* at 309 n.8.
361 *Id.* at 312.
362 *Keith*, 407 U.S. at 314–15.

domestic organizations; Plamondon himself was not the target.[363] A member of the defense team later speculated that Plamondon's calls from Algeria, where he was hiding, to the Oakland headquarters of the Black Panthers had been captured by an NSA intercept.[364] We will never know the details, because the government chose to dismiss the charges against Plamondon rather than disclose the surveillance records.[365] My point, however, is simply that foreign collection should not change the constitutional analysis when the government takes advantage of our global communications network to both harvest and analyze in bulk, vast amounts of metadata relating to the communications of U.S. persons who have "no significant connection with a foreign power, its agents or agencies."[366]

C. Applying Keith *to Bulk Collection of Domestic Communications Metadata*

Assuming that courts, applying *Keith*, recognize the synergy of privacy and speech when determining Fourth Amendment challenges to government surveillance programs, what difference would that recognition make with respect to the bulk collection of communications metadata? Would the First Amendment values associated with conversational privacy even come close to changing the Fourth Amendment balance of interests when the prevention of terrorist attacks is the government's countervailing concern? The answer, as is almost always the case with a balancing test, is "It depends."

First, consider the government's argument that the collection and later analysis of communications metadata does not rise to the level of a Fourth Amendment seizure or search because communicators have no reasonable expectation of privacy in the transactional information they share with their telecommunications providers. This claim, based on *Smith v. Maryland*, was the centerpiece of the government's constitutional defense of the former Section 215 program,[367] and, as described in Part I, has been cited by the government to justify the NSA's unlimited contact chaining of domestic metadata collected under EO 12333.[368]

---

363 *Id.* at 300 n.2.

364 *See* Morrison, *supra* note 339, at 296.

365 *See* Damren, *supra* note 339, at 8.

366 *Keith*, 407 U.S. at 309 n.8. Of course, Congress recognized this with respect to targeting of U.S. persons who are located abroad, which requires a FISA warrant. However, as explained in Part I, bulk collections of communications metadata are not covered under that provision. *See supra* notes 78–81 and accompanying text.

367 *See* ADMIN. WHITE PAPER, *supra* note 29, at 19–20.

368 *See supra* notes 96–97 and accompanying text.

As detailed in Part II, a strong case can be made under the Fourth Amendment, considered by itself, that the third party doctrine is both outdated and inaccurate with respect to our expectations of privacy in the digital age.[369] The assumption of the risk rationale on which *Smith* was based was highly questionable in 1979, and later changes in technology—which require us to create digital third-party trails to send an email, search the Internet, or use our cell phones—have eviscerated that rationale entirely. Justice Marshall's observation in his *Smith* dissent is even truer today: "It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[370] Some lower courts have begun to recognize the inadequacies of the third party doctrine in the context of cell-site location data, holding that government collection of location-tracking information for an extended period without a warrant violates cell-phone users' reasonable expectations of privacy.[371]

This conclusion, that citizens do not expect the government to use privately owned cell phones as digital tracking tools, makes good sense. It is even more reasonable for citizens to assume that the government will respect their right to conversational and associational privacy under the First Amendment. As shown in Part III, communications metadata is often just as revealing as the underlying messages themselves; studies show that the content/non-content distinction does not hold up.[372] Email and phone records provide private details about conversations and relationships that law-abiding citizens rightfully consider to be none of the government's business.[373] According to the *Keith* Court, both the public fear of pervasive government surveillance, and the potential for future abuse of collected data, present

369 *See supra* notes 155–80 and accompanying text.

370 Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

371 *See, e.g.*, United States v. Graham, 796 F. 3d 332, 355–61 (4th Cir. 2015), *reh'g granted en banc*, No. 12-4825, 2015 U.S. App. LEXIS 19064 (4th Cir. Oct. 28, 2015) (distinguishing Smith v. Maryland to hold that law enforcement must procure a warrant to obtain long-term cell site location records); In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 317–18 (3d Cir. 2010) (holding that third party doctrine does not apply to cell site location information generated by cell phone service providers). *But see* United States v. Davis, 785 F.3d 498, 511–12 (11th Cir. 2015), *cert. denied*, 84 U.S.L.W. 3257 (U.S. Nov. 9, 2015) (applying third party doctrine to hold that cell phone users voluntarily convey cell site location information to their service providers); In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 614–15 (5th Cir. 2013) (same).

372 *See supra* notes 204–215 and accompanying text.

373 *See* Pew 2014 Study, *supra* note 1, at 22 (finding that, following the Snowden disclosures, close to 80% of Americans agreed or strongly agreed that the nation should be concerned about government monitoring of phone calls and emails).

dangers to free expression that deserve weight in the Fourth Amendment analysis. By combining these First and Fourth Amendment interests against the eroding justifications for the third party doctrine, the Court should recognize that U.S. persons have a reasonable expectation of privacy in their communications metadata. Depending on one's overall view of the third party doctrine, either a benefit or a short-coming of the *Keith* approach is that it allows the Court to limit the third party doctrine in the communications context, without having to discard the doctrine in its entirety.

Determining that the collection and analysis of communications metadata constitutes a search and seizure within the meaning of the Fourth Amendment, however, does not mean that the government surveillance program necessarily is prohibited. The government will argue, as it did in the former Section 215 telephony metadata context,[374] that even if the third party doctrine does not apply, the government's interest in preventing foreign terrorism outweighs any minimal privacy interest associated with the collection and analysis of incidentally acquired domestic communications metadata under EO 12333. While the *Keith* Court reserved the question of whether the warrant clause is subject to a foreign intelligence exception,[375] the FISA Court of Review in 2008 recognized such an exception and applied a reasonableness test to reject a telecommunications company's Fourth Amendment challenge to a foreign intercept order.[376] Lower courts consistently have held that when the government collects information abroad concerning a U.S. person, a reasonableness test, rather than the warrant requirement, applies.[377] Even in the criminal law context, the Court in recent years has moved towards a "reasona-

374 *See* ADMIN. WHITE PAPER, *supra* note 29, at 21 ("The telephony metadata collection is also consistent with the First Amendment" because "the program does not collect the content of any communications and . . . the data may be queried only when the Government has a reasonable, articulable suspicion that a particular number is associated with a specific foreign terrorist organization.").

375 407 U.S. 297, 308–09, 321–22 (1972).

376 In re Directives [Redacted] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F. 3d 1004, 1011–13 (Foreign Intel. Surveillance Ct. of Rev. 2008).

377 *See, e.g.*, United States v. Stokes, 726 F.3d 880, 893 (7th Cir. 2013) (holding that with respect to extraterritorial search by U.S. agents of U.S. citizen's home, Fourth Amendment requires application of reasonableness test rather than warrant requirement); In re Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 167 (2d Cir. 2008) (finding that wiretapping and search of U.S. citizen's home that occurs overseas is governed by Fourth Amendment reasonableness standard, not warrant requirement); United States v. Peterson, 812 F.2d 486, 490 (9th Cir. 1987) (applying reasonableness test that considered U.S. agents' compliance with foreign law in Fourth Amendment calculation).

bleness view" of the Fourth Amendment,[378] pursuant to which it looks to the totality of the circumstances and balances the legitimate government interests served by the search against the individual interests involved.[379]

On the government's side of the ledger, the executive branch argues that surveillance conducted pursuant to EO 12333 serves the undeniably significant interest in the prevention of potentially catastrophic terrorist attacks.[380] According to the NSA, communications metadata collected under EO 12333 help the NSA to "understand where to find valid foreign intelligence information needed to protect U.S. national security interests in a large and complicated global network" and to "map communications between terrorists and their associates."[381] National security—the same interest that the government used to justify surveillance in *Keith*—and the fight against foreign terrorism repeatedly have been described by courts as interests of the highest magnitude.[382] As a result, the balancing exercise starts with a heavy hand on the scale in favor of the government.

These are the identical concerns, of course, that the government used to justify bulk collection of domestic telephony metadata under the former Section 215. Assuming for the sake of argument that collection under the former Section 215 amounted to a Fourth Amendment search or seizure, the Obama Administration defended the reasonableness of that program not only by reciting the government's weighty interest in terrorism prevention, but also by pointing to various privacy safeguards and minimization procedures with which the NSA was required to comply. For example, the govern-

---

378 *See* Lee, *supra* note 356, at 1134–35 (contrasting the Court's former "warrant preference view" of the Fourth Amendment with the current "reasonableness view").

379 *See, e.g.*, Samson v. California, 547 U.S. 843, 847–48 (2006) ("'[U]nder our general Fourth Amendment Approach' we 'examin[e] the totality of the circumstances' to determine whether a search is reasonable within the meaning of the Fourth Amendment." (quoting United States v. Knights, 534 U.S. 112, 118 (2001) (alteration in original)); Florida v. Jimeno, 500 U.S. 248, 250 (1991) ("The touchstone of the Fourth Amendment is reasonableness."); *see also* Amar, *supra* note 310, at 759 ("We need to read the [Fourth] Amendment's words and take them seriously: they do not require warrants, probable cause, or exclusion of evidence, but they do require that all searches and seizures be reasonable.").

380 *See* EO 12333, *supra* note 13, at Preamble. ("Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States.").

381 *See* NSA Memorandum, *supra* note 14, at 3.

382 *See, e.g.*, Holder v. Humanitarian Project, 561 U.S. 1, 28 (2010) ("Everyone agrees that the Government's interest in combating terrorism is an urgent objective of the highest order."); *In re Directives*, 551 F.3d at 1012 ("[T]he relevant governmental interest—the interest in national security—is of the highest order of magnitude.").

ment emphasized that FISC orders limited the NSA's ability to query or disseminate the collected metadata,[383] and the program was subject to monitoring by the FISC, Congress, the Department of Justice, and the intelligence community.[384] Likewise, in upholding bulk telephony metadata collection against a Fourth Amendment challenge, a federal district court cited executive, congressional, and FISC oversight as evidence of the program's reasonableness.[385] Opponents of the former Section 215 collection regime naturally disputed the adequacy of these safeguards to minimize privacy harms but, sufficient or not, they contributed to the overall reasonableness analysis.[386]

As described in Part I, when the NSA engages in foreign-based electronic surveillance, it incidentally acquires large numbers of U.S. person communications, including calls made by Americans to people in foreign countries, and communications among Americans that happen to transit through international cables, or are stored on backup servers located in foreign countries.[387] In both the criminal law and foreign intelligence contexts, however, the mere fact that non-pertinent communications are collected as part of authorized surveillance does not make the surveillance unreasonable.[388] Rather, courts look to the adequacy of minimization procedures whereby the government tries to avoid or ameliorate the privacy intrusions associated with those incidental interceptions.[389]

So, for example, in 2014 a federal district court held that warrantless surveillance under Section 702 of FISA was reasonable because FISA-approved targeting and minimization procedures adequately protected the privacy of U.S. persons whose communications were

383 ADMIN. WHITE PAPER, *supra* note 29, at 15, 21.

384 *Id.* at 4–5.

385 ACLU v. Clapper, 959 F. Supp. 2d 724, 757 (S.D.N.Y. 2013), *rev'd on other grounds*, 785 F.3d 787, 826 (2d Cir. 2015).

386 For a summary of the objections to the former Section 215 program minimization procedures, see Susan Freiwald, *Nothing to Fear or Nowhere to Hide: Competing Visions of the NSA's 215 Program*, 12 J. TELECOMM. & HIGH TECH. L. 309, 324–25 (2014).

387 *See supra* notes 79–88 and accompanying text.

388 *See, e.g.*, United States v. Kahn, 415 U.S. 143, 157–58 (1974) (finding that conversations collected between a named party and an unspecific party is allowed); In re Directives [Redacted] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1015 (Foreign Intel. Surveillance Ct. of Rev. 2008) (noting that incidental collections do not render the collection unlawful).

389 *See, e.g.*, Scott v. United States, 436 U.S. 128, 140–42 (1978) (examining the facts and circumstances of the wiretap to determine whether the minimization procedure were adequate); *In Re Directives*, 551 F.3d at 1015 (finding that the minimization procedures were adequate).

incidentally acquired.[390] In conducting the reasonableness analysis, the court also emphasized the existence of congressional, as well as FISC, oversight of the program based on specific statutory reporting requirements.[391] The court pointed to procedures limiting the retention and dissemination of foreign communications of or concerning U.S. persons, and requiring that the identity of U.S. persons be deleted in certain circumstances.[392]

But minimization procedures that apply to FISA-based surveillance, including the Section 215 domestic telephony metadata collection program as reconstituted by the Freedom Act, do not apply to signals intelligence gathered under EO 12333.[393] The NSA's EO 12333 surveillance activities are not subject to FISC approval or review, nor has Congress chosen to subject those activities to significant legislative oversight.[394] And while the Attorney General has approved minimization procedures that govern the NSA's collection, analysis, and retention of U.S. person information acquired pursuant to EO 12333 surveillance, as detailed in Part I, those procedures are much less robust with respect to the incidental acquisition, and later analysis, of domestic communications metadata than they are with respect to communication content.[395] For example, Part I showed how, although the Freedom Act limits the NSA's ability to contact chain Section 215 domestic telephony metadata out to two hops, under SPCMA, the NSA may contact chain EO 12333-collected metadata through U.S. person identifiers in an unlimited manner. And while the Freedom Act requires the NSA to purge metadata determined to be irrelevant to foreign intelligence, communication records obtained under EO 12333 may be retained by the government for at least five years.

Another critical factor in determining whether incidental collection is, in fact, reasonable under the Fourth Amendment is its scope.[396] Enormousness can negate reasonableness. The FISC rec-

390 United States v. Mohamud, No. 3:10-CR-00475-KI-1, U.S. Dist. LEXIS 85452, at *72–73 (D. Ore., June 24,2013).

391 *Id.* at *63–64.

392 *Id.* at *65–66.

393 *See* NSA Memorandum, *supra* note 14, at 2 ("Collection pursuant to EO 12333 is conducted through various means around the globe, largely from outside the United States, which is not otherwise regulated by FISA.").

394 *See* Watkins, *supra* note 74 (quoting head of the Senate Intelligence Committee as saying that Congress does not "sufficiently" oversee EO 12333 surveillance because it falls under executive authority).

395 *See supra* notes 89–110 and accompanying text.

396 *See e.g.*, PCLOB Section 702 Report, *supra* note 93, at 96 (stating that the scope of the incidental collection of U.S. persons' communications under Section 702 of FISA "raise

ognized this in 2011, when Judge John D. Bates refused to reapprove NSA targeting and minimization procedures with respect to targeted acquisition of foreign Internet communications pursuant to Section 702 of FISA.[397] The government had informed Judge Bates that, because of "technological challenges,"[398] the NSA had and would continue incidentally to acquire tens of thousands of wholly domestic emails that had been routed internationally and that had no direct connection to the surveillance target.[399] Judge Bates ordered the NSA to stop email collection until the process could be better tailored to satisfy the Fourth Amendment's reasonableness requirement,[400] stating that "[t]here surely are circumstances in which incidental intrusions can be so substantial as to render a search or seizure unreasonable."[401]

How much metadata relating to the communications of U.S. persons who have "no significant connection with a foreign power, its agents or agencies"[402] does the NSA collect pursuant to its authority under EO 12333? The NSA isn't telling, but press reports indicate the scope of collection is massive. For example, in 2013 the *Washington Post* reported that under EO 12333, the NSA collects "hundreds of millions" of email address books and instant-messaging "buddy lists" belonging to people around the world, including many Americans, as that data travels over international data routes.[403] Although two unnamed intelligence officials declined to estimate how many Americans' contact lists were swept up in the dragnet, they "did not dispute that the number is likely to be in the millions or tens of millions."[404] As Alvaro Bedoya noted on the *Just Security* blog, the volume of incidental collection of U.S. person communications under EO 12333

---

questions about whether its impact on U.S. persons pushes the program over the edge into constitutional unreasonableness"); Alvaro Bedoya, *Executive Order 12333 and the Golden Number*, JUST SECURITY (Oct. 9, 2014, 10:14 AM) (examining the reasonableness standard under the Fourth Amendment).

397 FISC Memorandum Opinion (FISA Ct., Oct. 3, 2011) (Bates, J.), http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.

398 *Id.* at 30.

399 *Id.* at 72.

400 *Id.* at 78–79.

401 *Id.* at 75.

402 *Keith*, 407 U.S. 297, 309 n.8 (1972).

403 Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST (Oct. 14, 2013), https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

404 *Id.*

appears to be much larger than the mere tens of thousands of U.S. email communications that concerned Judge Bates.[405]

The scope of incidental collection of American communications metadata under EO 12333 is also vital from a speech perspective. There is enormous First Amendment value in ensuring that major American communications systems—including telephone companies and Internet service providers—are not co-opted, infiltrated, or infected by the government in a way that threatens the sanctity of our citizens' communications.[406] Free speech and a free press are requisite components of a democratic system, and the existence of an "infrastructure of free expression"[407] creates the public trust needed for a democracy to function. That trust has been shaken by the Snowden revelations; it could be destroyed if citizens realize that, thanks to government overreaching under EO 12333, the Freedom Act's touted surveillance reforms are more illusory than real.[408] While whistleblower John Napier Tye[409] may have had only limited success so far at bringing EO 12333 to the attention of ordinary Americans, for all we know, the next Edward Snowden could be waiting in the wings.

Finally, any evaluation of Fourth Amendment reasonableness must also include a cost-benefit analysis. Privacy and speech concerns associated with pervasive government surveillance can only be outweighed by legitimate national security interests if, in fact, the program has value in the fight against terrorism. For this reason, after concluding that the former Section 215 program had not prevented any terrorist attacks,[410] the PCLOB called for a halt, and the Presi-

405 *See* Bedoya, *supra* note 396 (noting that the number of emails collected outnumber the tens of thousands that worried Judge Bates).

406 Documents leaked by Edward Snowden continue to reveal how the government has partnered with telecommunication companies to implement mass surveillance programs. For example, in August 2015, the *New York Times* and *ProPublica* reported that AT&T provided the NSA with access to billions of telephone and email records from 2001 to 2013. Julia Angwin, et al., *AT&T Helped U.S. Spy on Internet on a Vast Scale*, N.Y. TIMES, Aug. 16, 2015, at A1.

407 *See* Balkin, *supra* note 122, at 4 (describing the role of data processing systems in distributing the benefits of modern citizenship).

408 *See* Pew 2014 Study, *supra* note 1, at 23–25 (concluding that, following the Snowden disclosures, most Americans felt insecure sharing private information over landline phones, cell phones, email and social media.). The same study found that only 18% of American adults said they expect the federal government to do "the right thing" all or most of the time, and close to 80% agreed or strongly agreed that the nation should be concerned about government monitoring of phone calls and emails. *Id.* at 22, 28.

409 *See supra* notes 112–13 and accompanying text.

410 *See* PCLOB Section 215 Report, *supra* note 7, at 11 ("Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a con-

dent's Review Group on Intelligence and Communications Technology ("PRG") recommended significant reforms, to the former Section 215 telephony metadata collection program.[411] We can assume that overseas surveillance conducted under EO 12333 has provided the intelligence community with essential information over the years with respect to national security. However, the relevant inquiry here is whether the government's use of international methods to incidentally collect and analyze metadata associated with Americans' essentially domestic communications is justified in the fight against terrorism. Could the government use technology to limit its intake of American communications records under EO 12333 such that the program would still be effective? Does the NSA intentionally drive domestic Internet communications through international transit routes so as to collect it under EO 12333? Has the NSA thwarted any terrorist plots as a result of allowing enhanced analysis of U.S. person communications metadata under SPCMA? Given the secrecy surrounding EO 12333, we just don't know.

D. A Way Forward

Until the Supreme Court loosens the overly rigid standing requirements it adopted in *Clapper v. Amnesty International USA*,[412] a constitutional challenge to incidental collection of domestic communication records under EO 12333 is a virtual impossibility.[413] Nevertheless, given the important First and Fourth Amendment interests upon which such surveillance intrudes, both Congress and the executive branch can and should take steps to provide meaningful privacy protections with respect to EO 12333 collection and analysis of the communications records of U.S. persons. Below, I have listed some suggestions.

1. The public and Congress need more information regarding the scope of NSA surveillance conducted under EO 12333. The Snowden leaks trig-

crete difference in the outcome of a counterterrorism investigation."); PRG Report, *supra* note 85, at 104 ("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.").

411 *See* PCLOB Section 215 Report, *supra* note 7, at 168 (recommending to stop the Section 215 bulk telephone records program); PRG Report, *supra* note 85, at 115–29 (recommending several modifications to the Section 215 program such as changing the storage of the data from the government to a private third party).

412 133 S. Ct. 1138 (2013).

413 *See supra* notes 357–71 and accompanying text.

gered both official inquiries and public debate regarding the NSA's collection of bulk domestic telephony metadata under the former Section 215. As a result, Congress stepped in and, with the Freedom Act, imposed some important limits on that program. The democratic process worked. An unfortunate side effect of the Freedom Act, however, is that many Americans now believe—incorrectly—that their communications metadata are no longer being collected in bulk, held and analyzed by the NSA. Even worse, members of Congress similarly may be in the dark, given the pervasive secrecy surrounding the scope of incidental collections of American communications records under EO 12333. To the extent that national security allows, Congress and the American people need sufficient information regarding the scope and efficacy of metadata collection and analysis conducted under EO 12333 to determine whether the accompanying burden on our constitutionally guaranteed civil liberties is, in fact, justified.

As a possible first step, the PCLOB in 2014 announced its intention to examine two counterterrorism-related intelligence community activities governed by EO 12333. Its goal was to provide, by the end of 2015, two written, classified reports assessing the balance between each of those activities and privacy, as well as possible recommendations to enhance civil liberties.[414] Additionally, the PCLOB said it intends to release a public report explaining how the government uses EO 12333 and its implementing procedures to collect, retain, and disseminate information about U.S. persons.[415] It is, of course, impossible to know how much useful data the public report will present, or how receptive the executive branch will be to any reform suggestions contained in the classified reports. In 2013, the White House refused to adopt a PRG recommendation meant to apply to EO 12333 activities, stating that to do so would require "significant changes" to regular EO 12333 procedures.[416]

Another question that needs answering is the extent to which Congress and its relevant subcommittees are briefed regarding surveillance activities under EO 12333. Senator Dianne Feinstein, for-

414 *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., PCLOB EXAMINATION OF E.O. 12333 ACTIVITIES IN 2015, at 1 (2015), https://www.pclob.gov/library/20150408-EO12333_Project_Description.pdf (describing the Board's intended process for reviewing two counterterrorism related activities governed by EO 12333).

415 *Id.*

416 *See* Tye, *supra* note 111 (explaining that Recommendation 12 of the PRG Report was understood by the White House to be intended to apply to EO 12333, and that the President had no plans to implement the recommendation).

mer chair of the Senate Intelligence Committee, has said that the committee has not exercised "sufficient" oversight of those activities.[417] Accordingly, as it did with the Church Committee in the 1970s, Congress should hold hearings or otherwise investigate the scope of the NSA's incidental collection of domestic communications under EO 12333. If the Freedom Act is actually a "huge nothingburger"[418] for the privacy community, both Congressional leaders and the American people are entitled to know it.

2. Congress must enact further surveillance reforms. Certainly Congress has the power and the duty not only to investigate the extent of intelligence agencies' surveillance activities, but also to propose, enact, and update limits on those activities, as exemplified by passage of the original FISA as well as the Freedom Act.[419] However, restrictions placed by the Freedom Act on the NSA's ability to collect, analyze, and retain domestic communications metadata are meaningless if the NSA can conduct virtually the same activities under EO 12333. Accordingly, Congress should, to the extent possible, subject NSA metadata collection and analysis under EO 12333 to comparable limits imposed by the Freedom Act. In particular, given that the NSA under SPCMA can analyze metadata without establishing a reasonable, articulable suspicion that a particular phone number or email address is associated with international terrorism,[420] Congress should forbid the NSA from contact chaining through U.S. identifiers. The NSA should also be required promptly to destroy all domestic communication records determined to be irrelevant to foreign intelligence. Additionally, Congress should force the NSA to provide notice to criminal defendants when evidence to be used in court against them has been derived from EO 12333 surveillance, as it must with respect to surveillance under Section 702 of FISA.[421] Finally, Congress should also mandate that the Director of National Intelligence pro-

417 *See* Watkins, *supra* note 74 (detailing the expansion of NSA authority under EO 12333).

418 *See* Harris, *supra* note 71 (explaining that the Freedom Act, by forcing phone companies to hold on to records, does not suspend the NSA's record program).

419 In 2014, Congress set limits on how long intelligence agencies can retain data collected under EO 12333. *See* Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293, § 309, 128 Stat. 3990 (2014) (listing limitations on data retention). Following the Act's passage, Sen. Ron Wyden indicated that although those limits did not meaningfully restrict the NSA, the Act nevertheless created a precedent for Congress to impose a legislative framework on EO 12333 surveillance activities. *See* Ellen Nakashima, *Congress Sets Limits on Overseas Data Collection*, WASH. POST (Dec. 17, 2014), https://www.washingtonpost.com/world/national-security/congress-sets-limits-on-overseas-data-collection/2014/12/17/82972c6e-8558-11e4-a702-fa31ff4ae98e_story.html.

420 *See supra* notes 100–04 and accompanying text.

421 *See supra* note 299 and accompanying text.

vide an annual report to Congress—classified in whole or part, as necessary—regarding surveillance activities conducted under EO 12333, including a good faith estimate of the scope of NSA incidental collection of American communications.

3. The President should amend EO 12333 to reflect modern communications technology. EO 12333 was adopted in 1981, before development of the Internet and global telecommunications networks made national borders irrelevant with respect to Americans' ability to communicate. EO 12333 needs to be updated to reflect these new technologies, and to acknowledge that domestic communications do not lose their constitutional protections because they happen to be stored on a backup server located in a foreign country, or flow through an international cable on their way across town. In this regard, Presidential Policy Directive 28 (PPD-28), which indicates that "signals intelligence shall be as tailored as feasible,"[422] may be a step on the path to reform. Section one, "Principles Governing the Collection of Signals Intelligence," states as follows:

> Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities. The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion."[423]

Recall from Part I, however, that the NSA's definition of "collect" does not include contact chaining and other analysis of metadata.[424] And it is unclear how PPD-28 relates to EO 12333, given that a later footnote states that "this directive is not intended to alter the rules applicable to U.S. persons in Executive Order 12333."[425] Again, more information is needed to clarify whether and how PPD-28 applies to the collection and analysis of U.S. person communications metadata under EO 12333.

4. The Attorney General should reject SCPMA. Regardless of whether Congress enacts statutory limitations, the Attorney General should return the NSA to pre-SCPMA guidelines regarding the analysis of U.S. person communications metadata gathered under EO 12333. As described in Part I, prior to 2010, NSA analysts stopped contact chaining communications metadata when they encountered a U.S. person phone number or email address.[426] The Attorney General approved

422 PPD-28, *supra* note 79, at § 1(d).

423 *Id.* at § 1(b).

424 *See supra* notes 105–09 and accompanying text.

425 PPD-28, *supra* note 79, at § 4(a) n.9.

426 *See supra* notes 94–99 and accompanying text.

SPCMA based on the argument that U.S. persons have no reasonable expectation of privacy in communications metadata because of the third party doctrine[427]—a position that is outdated and inaccurate, especially when considered in light both the First and Fourth Amendment values associated with conversational privacy. Unless the NSA can demonstrate that unlimited contact chaining and other augmented analysis of U.S. persons' communications metadata has been instrumental in the nation's fight against terrorism, SPCMA will fail a Fourth Amendment reasonableness analysis that properly includes First Amendment interests in the balance.

5. The President should name a civilian to head the NSA. In its report on surveillance, the PRG suggested that greater civilian control of the NSA could increase its sensitivity to the privacy concerns of ordinary Americans.[428] It surmised that decisions regarding surveillance for counterterrorism purposes could be overly influenced by the combat needs of the military in Iraq and Afghanistan, especially considering that today, the same digital devices, operating systems, applications, routers, and fiber optic cables are used for both civilian and military communications.[429] While during military operations, surveillance directed towards our enemies must be "highly aggressive and largely unrestrained," the PRG noted that at home, the government must take care not to undermine communications privacy.[430] It recommended that the NSA director should be a Senate-confirmed position, and that the President should "give serious consideration" to appointing a civilian as the next NSA Director,[431] which would necessitate splitting off the U.S. Cyber Command military unit from the NSA—another one of the PRG's recommendations.[432]

Although the President reportedly had his staff draft a list of possible civilian candidates for the post when General Keith Alexander stepped down in 2014, the President ultimately appointed another military officer to lead the agency.[433] While I have no reason to doubt the qualifications or ability of Admiral Michael Rogers, it is telling that the *New York Times* immediately noted he had "no public track record in addressing the kind of privacy concerns that have put the

---

427 *Id.*

428 PRG Report, *supra* note 85, at 179–83.

429 *Id.* at 185–87.

430 *Id.* at 186–87.

431 *Id.* at 188.

432 *Id.* at 190.

433 David E. Sanger & Thom Shanker, *N.S.A. Choice Is Expert on Cyberwar*, N.Y. TIMES (Jan. 30, 2014), http://www.nytimes.com/2014/01/31/world/vice-admiral-to-be-named-nsa-director.html?_r=0.

agency under a harsh spotlight."[434] The idea that the government should develop different surveillance policies for military versus non-combat operations is worth future consideration. In that regard, the next head of the NSA should be a civilian who is subject to a Senate confirmation hearing where he or she must respond to elected representatives' concerns regarding agency overreach and the intrusions on privacy that accompany pervasive surveillance programs. This would both increase agency accountability, and help rebuild public trust in an agency thought by many to have drastically overstepped its bounds in the name of national security.

CONCLUSION

While no one can dispute the intelligence community's legitimate need to protect our nation, we must not forget Justice Powell's admonition that even when used sparingly, surveillance threatens our civil liberties and causes law-abiding citizens to distrust their government.[435] As technology evolves and our society becomes ever more dependent on digital devices, we can expect that massive government surveillance programs will continue to proliferate. If the government's surveillance power is left unchecked, we risk finding ourselves living in a world sociologists describe as the "surveillant assemblage," where law-abiding citizens who, in earlier times, were never the target of government surveillance, have become subject to routine monitoring.[436] The implications with respect to privacy, creativity, dissent, personal and political association, as well as the operation of a free press and our democratic processes, are enormous.

With the passage of the Freedom Act, Congress supposedly curbed the NSA's ability to spy on ordinary Americans by taking the agency out of the domestic metadata collection business entirely. In truth, however, the new law did nothing to limit the NSA's ability to capitalize on the global nature of modern communications networks to collect and analyze most of those same records in bulk under EO 12333. Both Congress and the public need more information about how, under EO 12333, the NSA scoops up and analyzes phone, email, and other communication records belonging not only to foreign ter-

434 *Id.*

435 United States v. U.S District Court, 407 U.S. 297, 312 (1972). *See supra* note 352 and accompanying text.

436 *See* Kevin D. Haggerty & Richard V. Ericson, *The Surveillant Assemblage*, 51 BRIT. J. OF SOCIOL. 605, 606 (2000) (describing how a "surveillant assemblage" transforms the purposes of surveillance to encompass individuals who formerly were not subjected to it).

rorists, but also to innocent Americans. Additionally, Congress should act to ensure that the intelligence community cannot use EO 12333 to evade statutory and constitutional protections by capturing Americans' communications from foreign sources.

Additional statutory and executive branch reforms are essential, given that under current Court precedent, a constitutional challenge to incidental collection of domestic communications metadata under EO 12333 might well fail. Even assuming that a litigant could overcome the near-insurmountable obstacles to standing imposed by *Clapper v. Amnesty International USA*,[437] courts in Fourth Amendment cases have applied the third party doctrine to hold that Americans have no reasonable expectation of privacy in their communications metadata. Alternatively, under First Amendment case law, government surveillance programs that do not target any particular group, or prohibit or punish speech, are unlikely to be seen as presenting an actionable chilling effect on speech or association.

My central theme has been that the First Amendment, when considered in partnership with the Fourth, can and should play a role in protecting us against becoming the surveillant assemblage. Both courts and the executive branch should avoid viewing the Bill of Rights as merely creating narrow, isolated zones of protection for our rights of privacy and speech. The risk with such an overly insular analysis, of course, is that a governmental activity that straddles the two constitutional provisions may simply fall into the resulting black hole between the constitutional guarantees. A better approach in addressing the momentous speech and communications privacy issues associated with bulk government surveillance programs would be to read the provisions of the First Amendment together with those of the Fourth. The First Amendment value of communications privacy must be factored into the determination of whether a government surveillance program violates the Fourth Amendment. As the Court demonstrated in the *Keith* case, when the two Amendments are taken in tandem, as pieces of the same cloth, they create a force field that extends the protections of each.

437 133 S. Ct. 1138 (2013). *See infra* notes 286–307 and accompanying text.