NOTES

SECRECY, STANDING, AND EXECUTIVE ORDER 12,333

CHARLOTTE J. WEN*

If my experience serves any purpose, it is to illustrate what most already know: courts must not be allowed to consider matters of great importance under the shroud of secrecy, lest we find ourselves summarily deprived of meaningful due process. If we allow our government to continue operating in secret, it is only a matter of time before you or a loved one find yourself in a position like I did - standing in a secret courtroom, alone, and without any of the meaningful protections that were always supposed to be the people's defense against an abuse of the state's power.

—Ladar Levison, founder of Lavabit[1]

* J.D. 2016, University of Southern California, Gould School of Law. With thanks to my friends and family for their unwavering support through law school, and to Professor David Cruz for his invaluable advice and guidance.

1. Ladar Levison, *Secrets, Lies and Snowden's Email: Why I Was Forced to Shut Down Lavabit*, GUARDIAN (May 20, 2014, 7:30 PM), http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email. Ladar Levison is the creator of Lavabit, an email service designed to subvert surveillance through the use of public-key encryption. *Id.* When the FBI became aware that Edward Snowden was using Lavabit to correspond with journalists, the FBI served Levison with a court order demanding that he turn over Lavabit's private encryption keys. *Id.* Levison fought the order in a top-secret proceeding and lost. *Id.* Determined not to compromise his customers' security, he complied with the order by submitting a printout of Lavabit's five encryption keys in eleven pages of four-point type. Motion for Sanctions at 2, *In re* Order Authorizing the Use of a Pen Register/Trap and Trace Device on an Electronic Mail Account, No. 1:13EC297 (E.D. Va. Aug. 5, 2013), https://www.documentcloud.org/documents/801182-redacted-pleadings-exhibits-1-23.html, at 141. When the FBI complained that it was illegible, Levison shut down the Lavabit service and was held in contempt of court. Kevin Poulsen, *Edward Snowden's E-Mail Provider Defied FBI Demands to Turn Over Crypto Keys, Documents Show*, WIRED (Oct. 2, 2013, 5:27 PM), http://www.wired.com/2013/10/lavabit_unsealed/. Levison appealed his case to the Fourth Circuit, which affirmed the district court's judgment. United States v. Lavabit, 749 F.3d 276, 279 (4th Cir.

You need the haystack to find the needle.

—General Keith B. Alexander, Director, National Security Agency[2]

TABLE OF CONTENTS

INTRODUCTION

In summer of 2013, the National Security Agency ("NSA") rocketed into headlines when Glenn Greenwald, a reporter at the *Guardian*, broke a stunning, Orwellian story: pursuant to top-secret court orders,[3] Verizon and other major telephone service providers had granted the NSA blanket access to their American customers' call records.[4] These companies,

2014).

2. J.D. Tuccille, *Why Spy on Everybody? Because "You Need the Haystack to Find the Needle," Says NSA Chief*, REASON.COM (July 19, 2013, 2:39 PM), http://reason.com/blog/2013/07/19/why-spy-on-everybody-because-you-need-th.

3. *See, e.g.*, Secondary Order at 2, *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc., No. BR 13-80 (FISA Ct., Apr. 25, 2013).

4. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 PM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. *See also Are They Allowed to Do That? A Breakdown of Selected*

Greenwald claimed, were providing the NSA with telephony metadata—general information about each of their customers' calls, such as phone numbers, call lengths, and call times.[5] In the face of the ensuing public outcry, the American government acknowledged the existence of the telephony metadata program.[6] In doing so, however, it was careful to assert that the program, while secret, was nonetheless constitutional, and that the court orders had been issued pursuant to the Foreign Intelligence Surveillance Act ("FISA").[7]

Documents then surfaced alleging the existence of two additional surveillance programs—PRISM and Upstream[8]—that, unlike the telephony metadata program, could be used to acquire the substantive *content* of American communications.[9] In response, James Clapper, the Director of National Intelligence ("DNI"), released a statement decrying the leaks as inaccurate.[10] Clapper insisted that the programs were constitutionally valid, arguing that FISA-authorized surveillance, including both PRISM and Upstream, was by law subject to judicial and congressional review. In the

Government Surveillance Programs, BRENNAN CTR. FOR JUSTICE AT THE N.Y. UNIV. SCH. OF LAW (July 15, 2013), https://www.brennancenter.org/analysis/are-they-allowed-do-breakdown-selected-government-surveillance-programs. The Patriot Act is an amendment to the Foreign Surveillance Intelligence Act ("FISA"), discussed *infra* Part I.A, which allows the government to apply for orders compelling the "production of tangible things" for the purposes of foreign intelligence investigations. Patriot Act § 215(a)(1) (2001), 50 U.S.C. § 1861(a) (2012).

5. Secondary Order, *supra* note 3, at 2. Many people, including both commentators and litigants challenging the telephony metadata program in the courts, have argued that government agencies can extrapolate personally identifying information from these call records—for example, cross-referencing them with cell phone geolocation data and credit card usage to track a person's movements and the identities of the people they are communicating with. *See, e.g.*, CITIZENFOUR (Praxis Films 2014) (depicting Occupy Wall Street activist and security expert Jacob Appelbaum discussing the implications of government acquisition of metadata and cell phone information).

6. It was most recently reauthorized on December 8, 2014. Verizon and other major phone companies continue to turn over call metadata of all of their American customers to the U.S. government. Press Release, U.S. Dep't of Justice, Joint Statement from the Office of the Attorney Gen. and the Office of the Dir. of Nat'l Intelligence on the Declassification of Renewal of Collection Under Section 501 of the Foreign Intelligence Surveillance Act (Dec. 8, 2014), https://www.justice.gov/opa/pr/joint-statement-office-attorney-general-and-office-director-national-intelligence.

7. Press Release, James Clapper, Dir. Of Nat'l Intelligence, DNI Statement on Activities Authorized Under Section 702 of FISA (June 6, 2013) [hereinafter Press Release, Clapper], http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa. *See* 50 U.S.C. § 1881a(h), (j) (2012) (provisions of FISA providing for limited judicial review); *infra* Part I.A.

8. *NSA Slides Explain the PRISM Data Collection Program*, WASH. POST (June 6, 2013), http://washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

9. *See id*. The slides reveal that PRISM collects email, chat (both video and voice), videos, photos, VoIP, file transfers, video conferences, notifications of target activity (login sessions), online social networking details, and other "special requests." *Id.*

10. Press Release, Clapper, *supra* note 7.

wake of these revelations, public debate about government surveillance became focused on FISA reform, with advocates pushing for more accountability and oversight.[11] The U.S.A. Freedom Act, a set of amendments to FISA, was introduced in both the House and the Senate.[12]

No more than a handful of months after these attempted FISA reforms were introduced, a disillusioned ex-State Department official, John Tye, penned an editorial in the *Washington Post* urging the American public to shift its focus from FISA to Executive Order 12,333 ("EO 12,333").[13] Tye wrote that EO 12,333, a relic of the Reagan administration, was being used to authorize "voluminous, unnecessary, and unconstitutional" amounts of American communications.[14] Tye stressed that merely reforming FISA could not by itself adequately address the public's concerns about the overreaches of government surveillance.[15] This was because EO 12,333, Tye explained, created a gaping "legal loophole," one "that allow[ed] the NSA to collect a huge amount of domestic U.S. communications to Americans, from Americans, by Americans just so long as those

11. *See, e.g.*, Denver Nicks, *Privacy Advocates Call for FISA Court Reform*, TIME (July 10, 2014), http://time.com/2970766/privacy-freedom-act-reform-secret-nsa-oversight-fisa/; Andrea Peterson, *The House Is Divided Over Almost Everything. But FISA Court Reform Might Be Able to Unite It*, WASH. POST (Oct. 1, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/10/01/the-house-is-divided-over-almost-everything-but-fisa-court-reform-might-be-able-to-unite-it/; Charlie Savage, *Changes to Surveillance Bill Stoke Anger*, N.Y. TIMES, May 21, 2014, at A20; *Foreign Intelligence Surveillance Act Reform*, EPIC, https://epic.org/privacy/terrorism/fisa/reform/ (last visited May 30, 2016).

12. Charlie Savage, *Senator's Bill is Stricter on N.S.A. Than House's*, N.Y. TIMES, July 25, 2014, at A20. The bill failed to pass the sixty-vote threshold in the Senate to reach debate on November 18, 2014 and will not move forward. Joe Mullin, *U.S. Senate Falls Two Votes Short of Shutting Down NSA Phone Spying*, ARS TECHNICA (Nov. 18, 2014, 4:55 PM), http://arstechnica.com/tech-policy/2014/11/us-senate-falls-2-votes-short-of-shutting-down-nsa-phone-spying/.

13. Exec. Order No. 12,333, 3 C.F.R. § 200 (1981), *reprinted in* 50 U.S.C. § 401 app. at 44–51 (1982) [hereinafter EO 12,333].

14. 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. Tye's assertion that the American public stopped focusing its attention entirely on FISA has been corroborated by Timothy Edgar, Obama's former director of privacy and civil liberties. Barton Gellman & Ashkan Soltani, *NSA Surveillance Program Reaches 'Into the Past' to Retrieve, Replay Phone Calls*, WASH. POST (Mar. 18, 2014), 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.

15. Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, N.Y. TIMES, Aug. 14, 2014, at A12. *See* Charlie Savage & Alicia Parlapiano, *Two Sets of Rules for Surveillance, Within U.S. and on Foreign Soil*, N.Y. TIMES (Aug. 13, 2014), http://www.nytimes.com/interactive/2014/08/13/us/two-sets-of-rules-for-surveillance.html (including a chart comparing types and breadth of surveillance authorized under FISA versus Executive Order 12,333).

communications are collected outside the borders of the United States."[16]

This "loophole," discussed further below,[17] consists of two components: (1) EO 12,333's granting of broad authority to the intelligence community to prescribe the scope of foreign surveillance allowed under the Order, including the ability to define words in the Order itself; and (2) the intelligence community's subsequent use of that authority both to increase its ability to collect American communications *and* to conceal that ability from the American public.[18] Essentially, EO 12,333 allows the intelligence community to grant itself authority to conduct foreign surveillance as it sees fit, with little to no oversight.

For example, EO 12,333 prohibits the intelligence community from targeting individual U.S. persons except in specific circumstances. It also authorizes the Department of Defense ("DOD")—an agency within the intelligence community—to "collect" foreign surveillance. The DOD, quite helpfully for itself, opted to define the point of "collection" not as the point at which the government *acquires* a particular communication by downloading or intercepting it, but rather when the communication is *received for official, sanctioned use*—that is, when a DOD analyst has already identified a target and officially requested the communication under internal procedures.[19] Thus, the DOD may collect and store an

16. Privacy and Civil Liberties Oversight Board, Transcript of Public Meeting 66–67 (July 23, 2014) [hereinafter PCLOB Public Meeting Transcript], https://www.pclob.gov/library/20140723-Transcript.pdf. John Tye provides a chilling example of the virtually unrestrained power that EO 12,333 authorizes:

> For example, we're here in Washington, D.C. and we're just a couple of blocks from the White House. Let's say hypothetically I was using Gmail, or Yahoo, or another big email provider, and sitting right here I sent an email to the President at that White House just two blocks away, it's almost certain that that email would be stored on servers around the world. So a lot of these server networks have mirror servers in countries like Brazil, Japan, South Korea, the United Kingdom, all over the world.
>
> So there's nothing in Executive Order 12333 that would prevent the NSA from collecting that email from here, two blocks away, and all such emails between U.S. persons in the United States.

Id. at 67–68.

17. *See infra* Part I.B.

18. DEP'T OF DEF., PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS (1982) [hereinafter DOD 5240.1-R]. DOD 5240.1-R is an internal, procedural implementation of EO 12,333 authority. As will be discussed *infra* Part I.B, the Order does not provide specific procedures or even meaningful guidelines for the government to follow. It merely vests broad, unspecific authority in intelligence community leaders to implement their own procedures for intelligence collection. *Id.*

19. *Id.* Edward Snowden has alleged that, at least in the NSA, intelligence analysts can access communications within the government database with the push of a button. *See* CITIZENFOUR, *supra* note 5. Snowden worked for the NSA as a systems administrator, which meant that he could access communications in the government database. This therefore raises the issue of whether a rogue or impatient analyst's unlawful access to the communications qualify as official, sanctioned use and

infinite number of American communications on its servers without ever having "collected" it under EO 12,333, so long as no intelligence analyst accesses the communication through official channels. It may even be the case that a rogue, impatient, or unscrupulous analyst's unsanctioned and unofficial access to a particular communication would not constitute "collection" under the DOD's guidelines.

The question becomes, then, what a concerned member of the American public can do if he or she believes that EO 12,333 infringes on his or her rights. The mind jumps rather naturally to the classic American recourse of litigation, litigation, and more litigation. There are fewer options to modify an executive order than a piece of legislation like FISA—while any member of Congress may introduce a new bill and push for reform, only the President can issue an executive order. Short of electing a presidential candidate intent on minimizing the surveillance state, the public has only one option: the judiciary. However, as this Note will show, it is nearly, if not actually, impossible for a person to challenge any surveillance authorized under EO 12,333 in the courts.

Part I introduces the legal particulars of FISA Section 702—the law used to authorize the telephony metadata program—and EO 12,333, and most importantly it highlights the differences between the two. It focuses on how Section 702 integrates judicial review into the process of issuing surveillance directives to communications service providers. It also elaborates on the legal "loophole" created by EO 12,333, and explains how EO 12,333 has created conditions ideal for unchecked and unlimited surveillance.

Part II provides background on the many court challenges to government surveillance that have failed because of the standing doctrine—specifically, the requirement that the plaintiff allege a concrete and particularized injury in fact. The reasons for this are legion—the Supreme Court's inconsistent and often baffling application of injury in fact jurisprudence, the inherently secret and classified nature of covert government surveillance, and the ability of the government to exercise the state secrets privilege to avoid verifying the existence of covert surveillance operations.

In Part III, I argue that EO 12,333 surveillance programs are essentially insulated from judicial review because of the immense difficulty that prospective plaintiffs face in attempting to allege an injury in fact. It

whether this unofficial, unsanctioned use would constitute "collection."

profiles *Schuchardt v. Obama*,[20] a case filed in 2015 questioning the constitutionality of the Order, to illustrate these challenges. Next, it describes how *Clapper v. Amnesty International USA*,[21] a 2013 Supreme Court decision, sets too high a bar for surveillance plaintiffs and must be changed. Out of respect for and in light of stare decisis, I argue that a future court can distinguish EO 12,333 challenges from the *Clapper* decision based on differences between FISA and EO 12,333.

I. THE MODERN REGIME: FISA AND EO 12,333

FISA[22] and EO 12,333 both serve as points of authority for foreign intelligence activities[23] and share some key similarities. For example, they are frequently used in conjunction with one another.[24] Both have received considerable media scrutiny.[25] Both govern foreign surveillance and intelligence collection[26] and impose limitations on the targeting of U.S. persons.[27] Despite these limitations, both programs have resulted in the substantial incidental collection of U.S. persons' communications.[28]

However, the lack of safeguards built into EO 12,333 becomes apparent when contrasted with FISA, which explicitly contains a number of

20. Schuchardt v. Obama, No. 14-705 (W.D. Pa. 2015).

21. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

22. Foreign Intelligence Surveillance Act § 702, 50 U.S.C. § 1881a (2012).

23. *The Surveillance Transparency Act of 2013: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 113th Cong. 98 (2013) [hereinafter *Surveillance Transparency Act Hearing*] (statement of Keith B. Alexander, Director, NSA) ("NSA conducts the majority of its SIGINT activities solely pursuant to the authority provided by Executive Order (EO 12333)").

24. *See, e.g.*, NAT'L SEC'Y AGENCY, CENT. SEC'Y SERV., SIGNALS INTELLIGENCE DIRECTORATE, UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE (1993) (describing the NSA's internal procedures for complying with FISA, EO 12,333, and Department of Defense Directive 5240.1-R—itself an implementation of FISA and EO 12,333).

25. *See, e.g.*, *supra* notes 4–12, 15, 16, 18; *NSA Surveillance Exposed*, CBS NEWS, http://www.cbsnews.com/feature/nsa-surveillance-exposed/ (last visited June 4, 2016); *In the News: NSA Surveillance*, L.A. TIMES, http://articles.latimes.com/keyword/nsa-surveillance (last visited June 4, 2016).

26. 50 U.S.C. § 1881(a) (2012); EO 12,333, *supra* note 13, at § 1.1(d).

27. 50 U.S.C. § 1881a(b) (prohibiting the use of FISA Section 702 in the targeting of persons located in the U.S.); EO 12,333, *supra* note 13, at §§ 2.3, 2.4 (prescribing limitations on collection and dissemination of information concerning U.S. persons, and requiring that any procedures used to direct surveillance against U.S. persons abroad be "the least intrusive collection techniques feasible").

28. Edward Snowden and John Tye have both alleged that FISA and EO 12,333 lead to the *incidental* collection of communications involving United States persons, though EO 12,333 does this on a greater scale. *See* Spencer Ackerman, *US Warned: Surveillance Reform Hinges on Change to Reagan Executive Order*, THE GUARDIAN (July 23, 2014, 4:44 PM), http://www.theguardian.com/world/2014/jul/23/nsa-surveillance-reform-reagan-order.

provisions for judicial review[29] in addition to a notification requirement[30] that may be used to facilitate surveillance plaintiffs' ability to allege injury in fact for standing.[31]

A. FISA SECTION 702

FISA Section 702 serves as the primary authority for the telephony metadata program, PRISM, and similar NSA surveillance programs.[32] At the time of the *Guardian* leaks, FISA allowed the intelligence community to request the FISA Court to order communications service providers to turn over the communications of any person reasonably believed to be outside the United States.[33] To do this, the FISA Court issues court orders, or "surveillance directives." These directives may only be issued to, and challenged by, service providers.[34]

1. Built-In Judicial Review and Its Limits

Under FISA, the government is not allowed to intentionally target U.S. persons or people known to be in the United States at the time of surveillance, nor may it skirt this prohibition by targeting people outside the United States with the ulterior motive of targeting someone inside it.[35] It is the intelligence community's responsibility to demonstrate to the FISA Court that this rule has been complied with.

While the FISA Court is the only entity that may issue surveillance directives, its ability to exercise discretion is relatively minimal; it is hamstrung by Section 702, which strictly dictates the scope of the court's review.[36] Essentially, the process works as follows. For each requested

29. 50 U.S.C. § 1881a(h), (j).

30. *Id.* §§ 1806(c), 1881e.

31. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147–55 (2013).

32. For an in-depth discussion on both the NSA's use of FISA and other legal authorities to justify its surveillance programs, as well as a detailed statutory analysis of FISA's various amendments and iterations, see Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 153–202 (2015).

33. 50 U.S.C. § 1881a(a). *See generally* Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1885c.

34. *In re* Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1009 (2008) (discussing the Protect America Act ("PAA"), which was a 2007 amendment to FISA). For more information about the PAA, see Donohue, *supra* note 32, at 135–37.

35. *See* 50 U.S.C. § 1881a(b)(1)–(4).

36. *Id.* § 1881a(h)–(i). The FISC is established in FISA Section 103. § 1803(a). It is also sometimes referred to as the "FISA Court." *See also* Tye, *supra* note 14 ("Bulk data collection that occurs inside the United States contains built-in protections for U.S. persons . . . . Such collection must be authorized by statute and is subject to oversight from Congress and the Foreign Intelligence Surveillance Court.").

surveillance directive, the Attorney General and DNI prepare three items for the FISA Court's review: (1) a signed certification that they reasonably believe that the proposed targets are not U.S. persons;[37] (2) "targeting" procedures, designed to limit the targeting of U.S. persons under the directive;[38] and (3) "minimization" procedures, designed to minimize the likelihood that the targets' identities will be exposed.[39] The court must then evaluate whether these items satisfy the requirements of both FISA and the Fourth Amendment.[40] If it decides that they are in compliance, it is then *required* by the text of Section 702 to issue the surveillance directive.[41] If the court decides that the request is defective, it must direct the government to correct the deficiency.[42]

Thus, Section 702 surveillance is by definition subject to judicial review, though the FISA Court's ability to exercise discretion in its determination of whether a surveillance directive may be issued is extremely limited by the text of the statute.

2. Notice and Fair Warning

In addition to the provision of limited judicial review, FISA provides an additional layer of protection for potential targets of Section 702 surveillance. If the Department of Justice ("DOJ") intends to use information obtained or derived from a surveillance directive against a defendant in a judicial or administrative proceeding, it is statutorily required to provide that defendant with "advance notice."[43]

However, it is worth noting that this requirement suffers from at least two limitations. First, the statute does not describe the nature of this "advance" notice—it provides neither a time frame nor a required method of delivery. Second, there is no way to enforce the notice requirement—indeed, despite Section 702's passage into law in 2008, the DOJ did not comply with the requirement until October 2013.[44]

37. *Id.* § 1881a(i)(2)(A).
38. *Id.* § 1881a(i)(2)(B).
39. *Id.* § 1881a(i)(2)(C).
40. *Id.* § 1881a(i)(3).
41. *Id.* § 1881a(i)(3)(A).
42. *Id.* § 1881a(i)(3)(B).
43. *Id.* § 1806(c).
44. Defendant's Reply in Support of His Motion for Disclosure of FISA-Related Material at 12, United States v. Daoud, No. 12-CR-00723 (N.D. Ill. Nov. 25, 2013), http://dig.abclocal.go.com/wls/documents/wls_112613_iteam_daoud%20filing%20fisa.pdf. *See also* Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. TIMES, Jul. 16, 2013, at A11.

B. EO 12,333

EO 12,333,[45] known in intelligence community parlance as "twelve triple three,"[46] was issued by President Ronald Reagan in 1981 to expand the foreign intelligence capabilities of the U.S. government.[47] At the time, three types of surveillance were off-limits under existing law: (1) communications by U.S. persons abroad; (2) U.S. persons' communications with persons abroad; and (3) any communications not consisting of "wire or radio."[48] Reagan signed EO 12,333 to fill in the gap created by the third excluded category, and EO 12,333 now serves as the authority for the majority of the NSA's interceptions of *electronic* communications.[49] It has laid a foundation for intelligence collection and oversight that has "prevailed ever since" it was established.[50]

1. The Structure of EO 12,333

EO 12,333 is comprised of three parts, each of which bears some responsibility for Tye's "legal loophole."

Part 1's primary purpose is to enumerate the various goals, powers, and responsibilities of the American intelligence community "elements," which are the various government agencies tasked with collecting intelligence in the national defense.[51] Part 1 authorizes more than half of these agencies to conduct covert surveillance operations and rests "ultimate responsibility" for producing intelligence and coordinating surveillance

45. EO 12,333, *supra* note 13.

46. Cyrus Farivar, *The Executive Order that Led to Mass Spying, as Told by NSA Alumni*, ARS TECHNICA (Aug. 27, 2014, 6:00 PM), http://arstechnica.com/tech-policy/2014/08/a-twisted-history-how-a-reagan-era-executive-order-led-to-mass-spying/.

47. Donohue, *supra* note 32, at 144–45.

48. *Id.* at 144 n.99.

49. *Surveillance Transparency Act Hearing*, *supra* note 23 ("NSA conducts the majority of its SIGINT activities solely pursuant to the authority provided by Executive Order (EO 12333)"). *See also* NAT'L SEC'Y AGENCY, LEGAL FACT SHEET: EXECUTIVE ORDER 12333 (2013), https://www.aclu.org/files/assets/eo12333/NSA/Legal%20Fact%20Sheet%20Executive%20Order%2012333.pdf; NAT'L SEC'Y AGENCY, LESSON 1 – INTRODUCTION (2007), https://www.aclu.org/files/assets/eo12333/NSA/Overview%20of%20Signals%20Intelligence%20Authorities.pdf (outlining an intelligence course about the authorities behind signals intelligence gathering).

50. Kevin W. Kapitan, *An Introduction to Intelligence Oversight and Sensitive Information: The Department of Defense Rules for Protecting Americans' Information and Privacy*, ARMY L., Apr. 2013, at 6.

51. EO 12,333, *supra* note 13. The Order names and individually delegates authority to fifteen intelligence community elements, and allows both the President and the DNI to designate new elements. *Id.* The elements include the usual suspects of the DOD, CIA, FBI, NSA, Department of State, and Department of Homeland Security, but also the intelligence bureaus of the Department of Energy and Department of the Treasury. *Id.*

collection with the DNI.

Part 1's primary contribution to Tye's "loophole" is the broad powers it vests in the DNI, Attorney General, and various intelligence community elements. For example, it authorizes the DNI to establish objectives for the entire intelligence community to ensure "timely and effective collection," guidelines for access to and dissemination of intelligence, and even new intelligence community elements or centers to address the priorities the DNI has established.[52] Most critically, the DNI's seventeenth enumerated power, ensconced between many others, is to "determine requirements and priorities for, and manage and direct the tasking, collection, analysis, production, and dissemination of, national intelligence . . . including approving requirements for collection and analysis."[53] Essentially, the Order vests this duty in a single unelected official, who is also permitted to delegate the responsibilities to whomever he or she chooses.[54]

Part 2 provides general guidelines for and limitations on the collection of surveillance under the Order, and addresses several critically important components of the loophole.[55]

First, it provides the intelligence community with vague powers and very little guidance as to how to exercise them. It authorizes the elements to "collect, retain, or disseminate" information regarding U.S. persons.[56] It imposes two primary "limitations" on this power: (1) the elements must respect the Constitution, especially the Fourth Amendment; and (2) the elements may only conduct surveillance activities by following procedures set forth by the DNI.[57]

Second, it provides an enumerated list of the types of information the elements may collect, many of which would easily encompass the communications of U.S. persons.[58] For example, in addition to obvious categories like information pertaining to terrorist and drug investigations, the Order may also be used to collect "[i]nformation concerning persons who are reasonably believed to be potential sources or contacts for the purposes of determining their suitability and credibility," as well as "[i]nformation necessary for administrative purposes."[59]

52. *Id.* § 1.3(b).
53. *Id.* § 1.3(b)(17).
54. *Id.* § 1.5.
55. *Id.* §§ 2.1–2.13.
56. *Id.* § 2.3.
57. *Id.* §§ 2.3–2.4, 2.8.
58. *Id.* § 2.3.
59. *Id.*

Third, it prescribes few limitations on collection. For example, it requires that surveillance against U.S. persons be conducted by the "least intrusive" means possible, but does not define what that means.[60] Additionally, it explicitly provides that no warrant is required for surveillance conducted under authority of the Order, even against a U.S. person, if the Attorney General believes there is probable cause that the U.S. person is an agent of a foreign power.[61]

Essentially, under the Order, surveillance may only be conducted in accordance with established procedure.[62] The Order does not provide further guidelines or impose any restrictions on the DNI's power to set these procedures. It merely vests in him or her the authority to do so.

Part 3 is comprised of miscellaneous provisions, including the only provision that addresses external oversight.[63] Instead of establishing a scheme for oversight, the Order merely acknowledges an existing statutory requirement, under the National Security Act, for the executive branch to keep Congress informed of its intelligence activities. It does not provide further guidance.[64] The reach of the National Security Act is limited—it does not require the intelligence community elements to obtain approval from the congressional committees prior to collecting intelligence.[65] Furthermore, the provision's lack of specificity has led to congressional intelligence committees receiving fewer information about EO 12,333 surveillance than they have other surveillance authorities.[66] As a result, Congress's oversight over EO 12,333 surveillance is limited in at least two respects: it is unable to stay apprised of EO 12,333 activities, and lacks the authority to direct or prevent intelligence collection.

2. The Other Half of the Loophole: Applications of EO 12,333

There is a limited amount of information available about implementations of EO 12,333 authority. Very few programs are matters of

60. *Id.* § 2.4.
61. *Id.* § 2.5.
62. *Id.* § 2.4.
63. *Id.* § 3.1.
64. 50 U.S.C. § 413(a) (2012); EO 12,333, *supra* note 13, at § 3.1.
65. 50 U.S.C. § 413(a)(2).
66. Press Release, Senator Dianne Feinstein, Feinstein Statement on NSA Compliance (Aug. 16, 2013), http://www.feinstein.senate.gov/public/index.cfm/2013/8/feinstein-statement-on-nsa-compliance ("The [Senate Intelligence] committee does not receive the same number of official reports on other NSA surveillance activities . . . conducted pursuant to legal authorities outside of FISA (specifically Executive Order 12333) . . . .").

public knowledge.[67] Many remain secret because the intelligence community has broad authority to conduct clandestine surveillance operations.[68] Whistleblowers like Edward Snowden and John Tye have revealed a small number of these implementations, while others have become public knowledge through voluntary governmental disclosures and Freedom of Information Act ("FOIA") lawsuits. Together, these revelations have shined a light on the systematic doublespeak responsible for Tye's "legal loophole."

Regulation 5240.1-R, for example, is the DOD's implementation of its EO 12,333 authority to create procedures governing the collection, retention, and dissemination of information about U.S. persons.[69] Internal DOD handbooks describe 5240.1-R as a "maze."[70] They advise budding analysts to tackle the Regulation by first "adjust[ing their] vocabulary."[71] 5240.1-R is one source of Tye's "loophole"—it defines "collection" as the point at which an intelligence community analyst "officially accepts, in some manner, such information for use within" his or her office or intelligence element.[72] Thus, when the government *incidentally* intercepts information about U.S. persons and stores it on government servers, it has not been legally "collected" within the meaning of 5240.1-R and, subsequently, the Order. The collection therefore would not violate the prohibition against collecting information relating to a known U.S. person.[73]

II. STANDING AND INJURY IN FACT IN THE MODERN ERA

In the wake of the September 11 attacks, the NSA initiated a massive policy shift in favor of warrantless surveillance.[74] However, the first public

67. *See generally* DOD 5240.1-R, *supra* note 18. According to Greg Nojeim, an attorney for the Center for Democracy and Technology, DOD 5240.1-R implements provisions of EO 12,333. PCLOB Public Meeting Transcript, *supra* note 16, at 48. Additionally, even though the regulation is publicly available, the DOJ has amended it in secret. *Id.*

68. Donohue, *supra* note 32, at 181.

69. DEF. INTELLIGENCE AGENCY, DOD HUMINT LEGAL WORKSHOP: FUNDAMENTALS OF HUMINT TARGETING 3 (2014), https://www.aclu.org/files/assets/eo12333/DIA/DoD%20HUMINT%20Legal%20Workshop%20Fundamentals%20of%20HUMINT%20Targeting.pdf; DOD 5240.1-R, *supra* note 18, at 15, 20, 22.

70. DEF. INTELLIGENCE AGENCY, INTELLIGENCE LAW HANDBOOK: DEFENSE HUMINT SERVICE 3–5 (2004), https://www.aclu.org/files/assets/eo12333/DIA/Intelligence%20Law%20Handbook%20Defense%20HUMINT%20Service.pdf

71. *Id.*

72. DOD 5240.1-R, *supra* note 18, at 15.

73. *See supra* note 27 and accompanying text.

74. Declaration of J. Kirk Wiebe in Support of Plaintiffs' Motion for Partial Summary Judgment Rejecting the Government Defendants' State Secrets Defense at 3, Jewel v. NSA, No. CV-08-04373-

exposé of these programs was not until December 2005, when the *New York Times* revealed that the NSA was spying on Americans without obtaining warrants.[75] Since then, many different classes of plaintiffs, including lawyers, humanitarian organizations, and telecommunications customers, have attempted and failed to challenge the constitutionality of both FISA and EO 12,333 in federal court.[76] And many, though not all, of these cases have been dismissed for lack of standing.[77]

Standing doctrine calls for federal courts to determine whether a plaintiff is "entitled to have the court decide the merits of the dispute" at hand.[78] The Court has developed constitutional and prudential requirements for standing.[79] To satisfy the constitutional requirements, plaintiffs must allege an injury that is "fairly traceable" to the defendant's actions and which would likely be redressable in the courts.[80]

Standing doctrine has been criticized by commentators and justices alike.[81] One chief critique is that the arbitrariness with which the Court has

JSW (N.D. Cal. Sept. 28, 2012). Wiebe was a former NSA employee. *Id.* at 1. He claimed that prior to 9/11, the NSA had been focused on complying with FISA. *Id.* at 3. Post-9/11, the NSA adopted a new policy: it could "circumvent federal statutes and the Constitution as long as there was some visceral connection to looking for terrorists." *Id.*

75. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html; James Risen & Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. TIMES (Dec. 21, 2005), http://www.nytimes.com/2005/12/21/politics/spying-program-snared-us-calls.html; Eric Lichtblau & James Risen, *Spy Agency Mined Data Trove, Officials Report*, N.Y. TIMES (Dec. 24, 2005), http://www.nytimes.com/2005/12/24/politics/spy-agency-mined-vast-data-trove-officials-report.html.

76. *See, e.g.*, *infra* Part I.B (discussing modern electronic surveillance cases); Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1145 (2013) (human rights organizations and attorneys); Jewel v. NSA, 673 F.3d 902, 905 (9th Cir. 2011) (AT&T customers); ACLU v. Clapper, 959 F. Supp. 2d 724, 730 (S.D.N.Y. 2013) (civil liberties organizations); Klayman v. Obama, 957 F. Supp. 2d 1, 11 (D.D.C. 2013) (consumers of Yahoo, Google, and Microsoft); Complaint for Declaratory Judgment, 28 U.S.C. §§ 2201 and 2202 at 2, Twitter v. Holder, No. 14-cv-4480 (N.D. Cal. Oct. 7, 2014) (service provider).

77. *See* discussion *infra* notes 106–107.

78. ERWIN CHEMERINSKY, FEDERAL JURISDICTION 55 (Vicki Been et al. eds., 6th ed. 2012) (quoting Warth v. Seldin, 422 U.S. 490, 498 (1975)).

79. *Id.* at 58–59.

80. Allen v. Wright, 468 U.S. 737, 751 (1984) (citing Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 38, 41 (1976)).

81. *See, e.g.*, *id.* (conceding that constitutional requirements for standing are not "susceptible of precise definition"); *id.* at 767 (Brennan, J., dissenting) (arguing that the majority's decision to dismiss a suit challenging a federal law prohibiting tax deductions for racially discriminatory private schools on standing grounds was a "cover" for their unwillingness to recognize the nature of the injury); Flast v. Cohen, 392 U.S. 83, 127–29 (1978) (Harlan, J., dissenting) (describing the majority's application of standing principles as "a word game played by secret rules"); Heather Elliott, *The Functions of Standing*, 61 STANFORD L. REV. 459, 466–68 (2008) (arguing that the standing doctrine does a "minimally adequate" and even "abysmal job" performing the functions—promoting separation of powers and determining the best litigant—assigned to it by the Court).

applied standing principles has led to a body of inconsistent precedent, which in turn provides insufficient doctrinal guidance to courts faced with new standing issues.[82] In particular, the Court's recent decision in *Clapper v. Amnesty International USA*, a case about post-9/11 NSA surveillance, has attracted criticism for adopting an unusually rigid interpretation of injury in fact.[83]

The injury in fact requirement has historically posed the most daunting obstacle for plaintiffs challenging government surveillance in the courts.[84] In the following Sections, this Note shows how the Supreme Court has been inconsistent in its analysis of concrete and particularized injuries in fact, and identifies the challenges that various surveillance plaintiffs have faced in demonstrating this prong of the standing test.

A. CONCRETE AND PARTICULARIZED INJURY IN FACT

Under the injury in fact requirement for standing, plaintiffs must allege an injury that is "concrete and particularized" and "actual or imminent," as opposed to "conjectural or hypothetical."[85] The Court first introduced this notion of "injury in fact" in 1970, with *Association of Data Processing Service Organizations, Inc. v. Camp* and *Barlow v. Collins*.[86] In

82. Evan Tsen Lee & Josephine Mason Ellis, *The Standing Doctrine's Dirty Little Secret*, 107 NW. U. L. REV. 169, 172–74 (2012) (pointing out that the polar-opposite treatment of injury in fact in "procedural" cases like FOIA suits and more typical civil suits suggests that the U.S. CONST. art. IIIArticle III, Section 2, § 2 "cases and controversies" clause applies differently to different categories of cases); Richard J. Pierce, Jr., *Is Standing Law or Politics?*, 77 N.C. L. REV. 1741, 1777–79 (1999) (pointing out that federal courts have treated cases with similar facts in different ways—varying between "broad, permissive, and probabilistic" approaches and "demanding" plaintiffs to demonstrate particular and imminent injuries). *But cf. Allen*, 468 U.S. at 751–52 (noting that even though standing principles may lack precise definitions, "in many cases the standing question can be answered chiefly by comparing the allegations of the particular complaint to those made in prior standing cases" (citing Los Angeles v. Lyons, 461 U.S. 95, 102–05 (1983)).

83. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1160–62 (2013) (Breyer, J., dissenting).

84. *See, e.g.*, *id.* at 1155 (dismissing a suit challenging the constitutionality of FISA Section 702 because plaintiffs failed to allege a cognizable injury); ACLU v. NSA, 493 F.3d 644, 648, 661–62 (6th Cir. 2007) (dismissing a suit challenging warrantless government surveillance in part because plaintiffs could not prove with certainty that they had been spied on); Pete Yost, *Appeals Court Takes on NSA Surveillance Case*, ASSOCIATED PRESS (Nov. 4, 2014, 10:07 PM), http://bigstory.ap.org/article/9e12a6b4510b42128e86f828b315087e/appeals-court-takes-nsa-surveillance-case (reporting on standing questions being raised in oral argument in *Klayman v. Obama*, 957 F. Supp. 2d 1, 9 (D.D.C. 2013), *rev'd*, 800 F.3d 559 (D.C. Cir. 2015), a suit filed by an activist attorney to enjoin NSA surveillance). *But cf.* Jewel v. NSA, 673 F.3d 902, 912–13 (9th Cir. 2011) (holding that plaintiffs in suit challenging warrantless government surveillance had standing).

85. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

86. Ass'n of Data Processing Serv. Orgs., Inc. v. Camp, 397 U.S. 150, 152 (1970); Barlow v. Collins, 397 U.S. 159, 163 (1970); Cass R. Sunstein, *What's Standing after* Lujan*? Of Citizen Suits, "Injuries," and Article III*, 91 MICH. L. REV. 163, 169–70 (1992).

these two companion cases, the Court abandoned the idea that the legal merits of a plaintiff's case were determinative of whether a plaintiff should have standing, and instead held that eligibility for standing should be determined based on facts pertaining to the legal quality of each claim.[87] The Court coined the "injury in fact" phrase in *Data Processing*,[88] but it was in *Barlow* that it characterized injury in fact as a "personal stake and interest" imparting "the concrete adverseness required by Article III."[89]

First, the injury must be actual, specific, and personally suffered.[90] In *Allen v. Wright*, the Court denied standing to a class of black parents challenging the IRS's practice of granting tax exemptions to racially discriminatory private schools.[91] The Court reasoned that the plaintiffs were claiming an injury arising from the "mere fact" that the exemptions facilitated the schools' ability to maintain their segregation policies.[92] It noted that such a racial stigmatization injury could be sufficient to show standing only if the plaintiffs were "*personally* denied equal treatment."[93] Here, however, the plaintiffs' children were not enrolled in the discriminatory schools in question.[94] The Court expressed concern that allowing the plaintiffs to move forward with their claim would allow any black plaintiff to sue any discriminatory school in any state.[95]

Second, the injury must be definite, concrete, and particularized. For instance, the plaintiffs in *Lujan v. Defenders of Wildlife* were environmental groups seeking an injunction to require that the government enforce the Endangered Species Act of 1973 beyond U.S. borders.[96] The Court, focusing on the fact that none of the plaintiffs could demonstrate that they had concrete plans or timelines in place to visit or observe the endangered animals, rejected the plaintiffs' arguments for being too abstract.[97] It dismissed them, with a stern reminder to the plaintiffs that

87. *Data Processing*, 397 U.S. at 153; Sunstein, *supra* note 86, at 185.

88. *Data Processing*, 397 U.S. at 152.

89. *Barlow*, 397 U.S. at 164.

90. *See, e.g.*, F. Andrew Hessick, *Standing, Injury in Fact, and Private Rights*, 93 CORNELL L. REV. 275, 299–306 (2008).

91. Allen v. Wright, 468 U.S. 737, 746, 753 (1984).

92. *Id.* at 746.

93. *Id.* at 755 (quoting Heckler v. Matthews, 465 U.S. 728, 739–40 (1984)) (emphasis added).

94. *Id*. at 755–56.

95. *Id.*

96. Lujan v. Defs. of Wildlife, 504 U.S. 555, 559 (1992). The Secretaries of Defense and the Interior had promulgated a joint regulation limiting enforcement of the Act to within the borders of the United States. *Id.* at 558–59. The plaintiffs also sought declaratory relief, wanting the Court to declare this joint regulation unconstitutional. *Id.* at 559.

97. *Id.* at 564.

standing was not an "ingenious academic exercise in the conceivable."[98] In doing so, the Court reaffirmed a relatively high bar for injury in fact, reasserting an emphasis on the concreteness and imminence requirements.[99]

As previously noted, the Court has been criticized by commentators for the inconsistent way that injury in fact doctrine has developed. Critics have identified several different "flavors" of injury in fact, ranging from probabilistic and purely risk-based, to rigid and particularized.[100] For instance, in 2010 the Court found in *Monsanto v. Geertson Seed Farms* that a group of alfalfa farmers alleged a sufficiently concrete injury by establishing that there was a "reasonable probability" that their crops would be infected by genetically modified alfalfa seed.[101] The Court pointed out that the "high potential" for contamination would force the farmers to periodically run tests to ensure that their seed had not been contaminated, in turn raising their costs and making their prices less competitive.[102] They also acknowledged the *preventive* measures that the farmers alleged they would need to take to prevent infection.[103] The Court found that the additional cost of these preventive measures were harms that the farmers would suffer regardless of whether their crops were actually contaminated, and therefore were sufficiently concrete.[104] *Monsanto* is notable because the farmers in that case alleged a similar set of injuries—present, future, and preventative—as the *Clapper* plaintiffs, and received opposite results.[105]

B. INJURY IN FACT IN POST-9/11 DRAGNET SURVEILLANCE CASES

In recent years, the injury in fact prong of standing has been a silver bullet to many court challenges to post-9/11 NSA surveillance. The first lawsuits challenging this new brand of NSA surveillance, *Center for*

98. *Id.* at 566 (quoting United States v. Students Challenging Regulatory Agency Procedures, 412 U.S. 669, 688 (1973)).

99. Sunstein, *supra* note 86, at 226–28.

100. *See, e.g.*, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1134, 1161–63 (2013) (Breyer, J., dissenting) (providing a brief overview of cases in which the federal courts have accepted probabilistic injuries in fact to establish standing); Duke Power Co. v. Carolina Envtl. Study Grp., Inc., 438 U.S. 59, 75 n.20 (1978) ("Our recent cases have required no more than a showing that there is a 'substantial likelihood' that the relief requested will redress the injury claimed to satisfy the second prong of the constitutional standing requirement." (citations omitted)).

101. Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 153–56 (2010).

102. *Id.* at 154.

103. *Id.* at 154–55.

104. *Id.* at 155.

105. *See* discussion *infra* Part I.B.2.

Constitutional Rights v. Bush, *ACLU v. NSA*, *Hepting v. AT&T*, and *Al-Haramain v. Obama*, were filed in early 2006, followed by *Amnesty International v. Clapper* and *Jewel v. NSA* in 2008.[106] While *Jewel* is still in progress, the others have all been dismissed. Four of the cases—*ACLU v. NSA*, *Al-Haramain*, *Center for Constitutional Rights*, and *Clapper*—were dismissed at the federal appellate level for failure to establish standing.[107] Even *Jewel* was initially dismissed at the district court level on standing grounds.[108] A number of more recent cases, including *ACLU v. Clapper*, *Smith v. Obama*, and *Klayman v. Obama*, await federal circuit court decisions, also on the standing issue.[109]

The fatal flaw in surveillance plaintiffs' cases has overwhelmingly been their inability to allege a concrete and imminent injury in fact. Surveillance plaintiffs have advanced multiple theories of injury, including past, present, and future privacy violations for Fourth Amendment claims, as well as "chilling-effect" First Amendment claims. The past privacy violation theory has only been successfully argued at the federal appellate level once, by the plaintiffs in *Jewel v. NSA*, a Ninth Circuit case.[110] The Sixth Circuit and the Supreme Court have both rejected surveillance

106. *See generally* Ctr. for Constitutional Rights v. Bush, No. 07-CV-1115-VRW (N.D. Cal. 2006), *aff'd sub nom*. *In re* NSA Telecomms. Records Litig., 522 F. Appx. 383, 384 (9th Cir. 2013); ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007); Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006); Al-Haramain Islamic Found. v. Bush (Al-Haramain I), 507 F.3d 1190 (9th Cir. 2007); Al-Haramain Islamic Found. v. Obama (Al-Haramain II), 705 F.3d 845 (9th Cir. 2012) (*Al-Haramain II* is noted here because it was a continuation of the proceedings in *Al-Haramain I*; however, the legal issues at hand concerned sovereign immunity, not standing); Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013); Jewel v. NSA, No. C-08-CV-4373, 2010 U.S. Dist. LEXIS 5110 (N.D. Cal. Jan. 21, 2010), *rev'd*, 637 F.3d 902 (2011).

107. *ACLU*, 493 F.3d at 652–53 (see discussion *infra* Part I.B.1); *In re NSA*, 522 F. Appx. at 384–85 (holding that the plaintiffs had alleged an identical theory of injury as the plaintiffs in *Clapper v. Amnesty International USA*, and thus they did not have standing to sue); *ACLU*, 493 F.3d at 687 (holding that the plaintiffs failed to allege particularized injuries for each of their six asserted claims); *Al-Haramain I*, 507 F.3d at 1197 (holding that the state secrets privilege both blocked the assertion of the claim and made it impossible for plaintiffs to show standing); *Clapper*, 113 S. Ct. at 1143 (holding that the plaintiffs lacked standing). The plaintiffs in *Hepting* successfully alleged injury in fact. *Hepting*, 439 F. Supp. 2d at 1001. However, the suit was thrown out by the Ninth Circuit after Congress passed the FISA Amendments Act of 2008, which included an immunity provision protecting "any person . . . providing assistance to an element of the intelligence community" from civil suit. Hepting v. AT&T Corp., 539 F.3d 1157, 1157 (9th Cir. 2008); FISA Amendments Act of 2008, Pub. L. No. 110-261, 112 Stat. 2435, 50 U.S.C. § 1885a. The provision immunized service providers from suit, but not government actors. *In re* NSA Telecomms. Records Litig., 671 F.3d 881, 892 (9th Cir. 2011).

108. *Jewel*, 673 F.3d at 905. *See* discussion *infra* Part II.B.2.

109. ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); Smith v. Obama, 24 F. Supp. 3d 1005 (D. Idaho 2014), *vacated*, 816 F.3d 1239 (9th Cir. 2016); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013), *rev'd*, 800 F.3d 559 (D.C. Cir. 2015).

110. *See infra* Part II.B.2.

plaintiffs' proposed theories of present and future privacy violations on the grounds that they were unable to show with enough certainty that their communications had been or would imminently be intercepted by the government.[111] Chilling effect injuries have been rejected for being both self-imposed and just as tenuous as the present and future privacy violations.[112]

1. Surveillance Injuries

The plaintiffs in *ACLU v. NSA* were attorneys, journalists, nonprofit humanitarian organizations, and scholars who communicated frequently with people outside of the United States.[113] Their contacts were all people with significant knowledge of foreign issues and their conversations would undoubtedly be considered valuable foreign intelligence information. They brought six claims for declaratory and injunctive relief, challenging the validity and constitutionality of several surveillance programs and authorities.[114] The Michigan district court, taking a comparatively relaxed approach to injury in fact, found that the plaintiffs' plans to continue to engage in international communications, coupled with the NSA's real, ongoing, and certain-to-be-reauthorized surveillance of overseas communications, constituted an actual, imminent, concrete, and particularized injury and allowed the case to move forward.[115] On appeal, the Sixth Circuit disagreed.[116]

The Sixth Circuit opinion identified three primary theories of injury in the plaintiffs' standing argument: a "chilling effect" on the plaintiffs, a chilling effect on the plaintiffs' overseas contacts, and the NSA's violation of the plaintiffs' reasonable expectation of privacy.[117] The Sixth Circuit found that the alleged "chill" on the plaintiffs' speech was not a cognizable injury in fact for two reasons. First, the chill was "mere[ly] subjective"—it

111. This Note does not address the question of whether the government's incidental collection of private communications would actually constitute a violation of either the Fourth Amendment or due process.

112. *See infra* notes 117–120 and accompanying text.

113. Complaint for Declaratory and Injunctive Relief at 2, ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006) (No. 2:06-CV-10204).

114. ACLU v. NSA, 493 F.3d 644, 652–53 (6th Cir. 2007). The three constitutional claims were under the First Amendment, Fourth Amendment, and separation of powers doctrine, and the three statutory claims were under FISA, the Administrative Procedure Act, and Title III. *Id.* Title III refers to the federal electronic surveillance statutes codified at 18 U.S.C. §§ 2510–22. *Id.* at 679.

115. ACLU v. NSA, 438 F. Supp. 2d 754, 770 (E.D. Mich. 2006), *rev'd*, 493 F.3d 644 (6th Cir. 2007).

116. *ACLU*, 493 F.3d at 657.

117. *Id.* at 653–55.

rose out of the plaintiffs' subjective apprehension of *possible*, but not confirmed, government surveillance.[118] Second, the resulting "chill" on communications was purely "self-imposed," rather than imposed by the government defendants.[119] The Sixth Circuit did not determine whether the second chilling effect—that of the overseas contacts' speech—was an injury in fact.[120]

The Sixth Circuit did agree that the NSA's alleged violation of the plaintiffs' reasonable expectation of privacy in their overseas communications could be a "direct and personal" invasion.[121] However, the plaintiffs would still need to demonstrate "proof of such invasion"—that is, "demonstrate that [their] privacy had actually been breached."[122] Unfortunately for the plaintiffs, "no single plaintiff . . . [could] show that he or she [had] actually been wiretapped," so they could not demonstrate an injury.[123] The plaintiffs tried to have the court compel the government to release documents that could confirm or deny whether they had been wiretapped, but the government successfully invoked the state secrets privilege to prevent disclosure of any such information.[124] Under these circumstances, the Sixth Circuit ultimately found that the plaintiffs could not establish standing for any of their constitutional claims.[125]

This demanding injury in fact analysis was subsequently echoed by the Supreme Court in *Clapper*, the controversial case in which a group of attorneys and human rights organizations sued to enjoin surveillance authorized by FISA Section 702.[126] Like the plaintiffs in *ACLU v. NSA*, they claimed that Section 702 compromised their ability to communicate confidentially with witnesses and clients abroad.[127] Additionally, they argued that they had taken costly preventive measures to ensure the confidentiality of their international communications, and demanded relief

118. *Id.* at 663. The Sixth Circuit additionally noted that First Amendment chilling effect claims require the plaintiffs to be subject to a *direct* government regulation, order, or constraint, which was not the case for the *ACLU* plaintiffs. *Id.* (citing Laird v. Tatum, 408 U.S. 1, 11 (1972)).

119. *Id.* at 668–69.

120. *Id.* at 665–66. The Sixth Circuit found that the issue was not guided by clear precedent and that it would nonetheless not be determinative of standing in the instant case because the plaintiffs could not establish causation and redressability. *Id.*at 666.

121. *Id.* at 655.

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.* at 673, 675.

126. *See* Elisa Sielski, Clapper v. Amnesty International: *Who Has Standing to Challenge Government Surveillance?*, 8 DUKE J. CONST. L. & PUB. POL'Y 51, 52–54 (2013).

127. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1145 (2013).

from the government in the form of monetary damages.[128] The plaintiffs advanced two theories to show standing. First, they argued under a theory of future injury that there was an "objectively reasonable likelihood" that their communications would be acquired under Section 702 in the future.[129] Second, they argued that the costly preventive measures they had adopted constituted a present injury, since those costs were a direct result of the government's surveillance policies.[130] The Southern District of New York rejected both those theories, finding that the plaintiffs had only demonstrated an "abstract fear" that was insufficient to show injury in fact.[131] On appeal, the Second Circuit reversed, finding that although the future injury theory was too "probabilistic" and had not reached the proper threshold of likelihood, the present injury theory was an economic injury so "mundane" that it was surely sufficient to establish injury in fact for standing.[132]

The Supreme Court, in a 5–4 decision, reversed again, and held that the plaintiffs lacked standing to move forward on any of their claims.[133] Harkening back to the "concrete and particularized" requirements for injury in fact articulated in *Lujan*, the Court found that the plaintiffs' assertion that there was an objectively reasonable likelihood that their communications would be intercepted in the future was "too speculative" and not "certainly impending."[134] This conclusion, however, would appear to be at odds with *Monsanto*, in which the Court had applied a different standard for future harms: that is, the plaintiff need only demonstrate a "substantial risk"[135] or "reasonable probability"[136] of harm. The Court made very little attempt to justify the application of the new "certainly impending" standard to Amnesty International's future harms, as opposed to the "significant risk" and "reasonable probability" analysis from *Monsanto*. It only restated *Monsanto*'s facts—that the government's

128. *Id.* at 1143.

129. *Id.*

130. *Id.*

131. Amnesty Int'l USA v. McConnell, 646 F. Supp. 2d 633, 644–58 (S.D.N.Y. 2009), *aff'd sub nom*. *Clapper*, 133 S. Ct. at 1155. *See* Lexi Rubow, *Standing in the Way of Privacy Protections: The Argument for a Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action*, 29 BERKELEY TECH. L.J. 1007, 1017–19 (2014) (advancing different conceptualizations of possible cognizable privacy harms).

132. Amnesty Int'l USA v. Clapper, 638 F.3d 118, 133 (2d Cir. 2011), *rev'd sub nom*. *Clapper*, 133 S. Ct. at 1155.

133. *Clapper*, 133 S. Ct. at 1143.

134. Lujan v. Defs. of Wildlife, 504 U.S. 555, 565 n.2 (1992).

135. *Clapper*, 133 S. Ct. at 1160 (Breyer, J., dissenting).

136. *Id.* at 1143.

deregulation of alfalfa led to a "significant risk" of contamination, which was in turn supported by evidence that the plaintiffs' farms were in an area "well within" pollination range.[137] Then, without further explanation as to why the analysis could not apply in *Clapper*, the majority held that the *Clapper* plaintiffs' risk of injury was not as "concrete" as the alfalfa farmers in *Monsanto*.[138]

The majority went on to say that even if Amnesty International could demonstrate that government interception of their communications was "certainly impending"[139]—a standard that the Court had never before used to deny standing—they likely could not establish that the injury was directly traceable to the specific law being challenged—that is, Section 702 of FISA.[140] Essentially, the plaintiffs' theory required assuming as true several allegations that could not be proven: (1) that their contacts abroad would be targeted by the NSA under the authority of FISA Section 702; (2) that the FISA Court would authorize the targeting; (3) that the NSA would actually intercept their contacts' communications; and (4) that the plaintiffs' communications would be among those intercepted.[141]

The dissent, on the other hand, argued that the plaintiffs in *Clapper* and *Monsanto* presented "virtually identical circumstances."[142] In both cases, the plaintiffs, after assessing the risk of harm to their interests, made a decision to undertake measures to prevent that harm.[143] In both cases, there was significant risk that the plaintiffs would be subjected to the harms they were asserting. The dissent profiled several of the plaintiffs, pointing out that each communicated with their overseas contacts about politically sensitive information falling under the definition of "foreign intelligence" as defined by FISA[144]—as their contacts included Guantanamo Bay prisoners, terrorism suspects, political detainees, political activists, and journalists.[145] These contacts arguably were already on the intelligence community elements' radar as potential surveillance targets since the

137. *Id.* at 1153–54.
138. *Id.* at 1154.
139. *Id.* at 1151.
140. *See id.*
141. *Id.* at 1148–49.
142. *Id.* at 1164 (Breyer, J., dissenting).
143. *Id.*
144. *See* 50 U.S.C. § 1801(e) (2012) (defining "foreign intelligence information" as information that relates to the ability of the United States to protect against attacks, hostile acts, or terrorism, or that otherwise relates to national security or foreign affairs). The communications between terrorism suspects, former and present Guantanamo Bay prisoners, and political activists abroad and their attorneys would surely fall under this umbrella definition.
145. *Clapper*, 133 S. Ct. at 1157 (Breyer, J., dissenting).

government has a "strong motive" to learn as much as it can about suspected terrorists and Guantanamo Bay prisoners.[146] The majority did not address any of these arguments.[147]

The *Clapper* majority then rejected the plaintiffs' allegation that they had suffered a present injury in incurring substantial costs to implement preventive measures to protect their communications.[148] It held that the plaintiffs "cannot manufacture standing by choosing to make expenditures based on hypothetical future harm."[149] However, recall that the Court considered the *Monsanto* farmers' strongest alleged injury to be the preventative measures they planned to and did take to mitigate the "reasonable" threat of seed contamination.[150] Those farmers could surely also be accused of making expenditures based on hypothetical future harms. However, the majority made no effort to reconcile this discrepancy, adding more confusion to an already confused doctrine. Commentators have suggested that future courts will construe *Clapper* such that this heightened requirement only applies in cases involving national security.[151] But in any case, with this decision, the Court set a high standard for injury in fact in government surveillance cases, arguably narrowing the entryway for future surveillance plaintiffs.[152]

In the end, the *Clapper* majority addressed the plaintiffs' concern that denial of standing would insulate FISA Section 702 from judicial review, articulating two reasons why this was not the case.[153] First, the majority said, the FISA Court had been established for the express purpose of

146. *Id.* at 1158.

147. *See id.* at 1142–55.

148. *Id.* at 1143.

149. *Id.*

150. Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 153–55 (2010).

151. Note, *Standing — Challenges to Government Surveillance —* Clapper v. Amnesty International USA, 127 HARV. L. REV. 298, 298 (2013) [hereinafter *Standing*]. However, this argument is peculiar, because balancing government interests in national security versus individual interests in privacy seems to be a question that should arise within the context of a substantive Fourth Amendment claim. Standing, as discussed *supra* Part II.A, is largely about the plaintiff's right to appear in court in the first place.

152. *See* Patrick Gallagher, *Environmental Law,* Clapper v. Amnesty International USA*, and the Vagaries of Injury-In-Fact: "Certainly Impending" Harm, "Reasonable Concern," and "Geographic Nexus*," 32 UCLA J. ENVIRON. L. & POL'Y 1, 4 (2014) (arguing that *Clapper* muddied "an already confusing body of law" by confusing the "certainly impending" test with that of "reasonable concern"); *Standing*, *supra* note 151, at 303 (arguing that the "certainly impending" requirement standard was left unclear by *Clapper*, and must be read narrowly because of its likelihood of excluding "numerous litigants" from the courts).

153. *Clapper*, 133 S. Ct. at 1154–55.

hearing challenges to surveillance directives.[154] Thus, all surveillance orders issued under FISA authority were subject to judicial review by default. Second, FISA's advance notice requirement would enable a person who received such notice to allege with certainty that the government had collected his communications, and thus would have a "stronger evidentiary basis for establishing standing" than these plaintiffs.[155]

Notably, however, the majority only came to this conclusion as a direct result of Solicitor General Donald B. Verrilli's promises to that effect in oral argument.[156] *Clapper* was argued in October 2012.[157] However, the first time the DOJ actually used the notice requirement was a year later, in October 2013[158]—suggesting either that the DOJ had never used evidence obtained from FISA surveillance in any type of criminal proceeding prior to October 2013, or that they had not been complying with the law until October 2013.[159] It would follow that the surveillance plaintiff's path to alleging a proper injury in fact is much more difficult than the *Clapper* majority would suggest.

2. Challenging Demonstrated Surveillance

To date, *Jewel v. NSA* is the only case challenging post-9/11 NSA surveillance that has been considered on its merits after surviving an appellate-level evaluation of the plaintiffs' standing.[160] Unlike the *Clapper* and *ACLU* plaintiffs, the *Jewel* plaintiffs challenged the constitutionality of the NSA's actions themselves rather than a specific authority like FISA Section 702 or EO 12,333.[161] *Jewel* was a class-action lawsuit initially filed in 2008 by the Electronic Frontier Foundation seeking damages and to enjoin the U.S. government's collection of telephony data from customers of AT&T in San Francisco.[162] The plaintiffs had undisputed evidence that

154. *Id.*

155. *Id.* at 1154.

156. Liptak, *supra* note 44.

157. *See* Transcript of Oral Argument at 1, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1134 (2013) (No. 11-1025) [hereinafter Oral Argument, *Clapper*].

158. *See* sources cited *supra* note 44.

159. While this is not the topic of this Note, the DOJ's reluctance to comply with the statutory notice requirement suggests that the American public is not as protected by FISA as the *Clapper* majority seemed to believe.

160. While the Second Circuit did find that the *Clapper* plaintiffs had standing to sue, this was overruled by the Supreme Court. *Clapper*, 133 S. Ct. at 1155.

161. Jewel v. NSA, 673 F.3d 902, 905–06 (9th Cir. 2011). The plaintiffs claimed that the NSA's spying practices violated the First and Fourth Amendments, separation of powers, FISA, the Electronic Communications Privacy Act, the Stored Communications Act, and the Administrative Procedure Act. *Id.* at 906.

162. Complaint at 4, Jewel v. NSA, No. C-08-CV-4373 (N.D. Cal. Sept. 21, 2008).

AT&T had routed all consumer traffic to a "secret room in San Francisco controlled by the NSA."[163] Thus, they could definitively show that their communications and Internet usage had been intercepted.

The plaintiffs' injury in fact was so obviously actual and concrete that neither party made any standing arguments in briefs.[164] Nonetheless, the district court took up the standing issue *sua sponte* and dismissed the case on prudential principles, ruling that the injury was a generalized grievance not "sufficiently particular" to establish standing.[165]

On appeal, the Ninth Circuit rejected the district court's standing analysis.[166] The panel stressed that injuries must be "abstract and indefinite" to be generalized grievances.[167] The plaintiffs had been "highly specific" in laying out "concrete harms" arising from the government's actions.[168] Essentially, the plaintiffs had concrete proof, so they also had a concrete injury.[169] The court also made special note of the fact that the plaintiffs' lawsuit focused specifically on AT&T rather than being a "scattershot incorporation of all major telecommunications companies" or a "blanket policy challenge."[170] Although *Jewel* predated *Clapper* and the Supreme Court did not cite the case or any Ninth Circuit decision in their opinion, it nonetheless suggests that the courts do not welcome non-specific blanket challenges.

Similarly, the plaintiffs in *Klayman v. Obama*, currently being appealed to the D.C. Circuit, are challenging the constitutionality of a specific NSA program—bulk metadata collection from Verizon—rather than the underlying authorities.[171] The district court found that the plaintiffs had standing because they had "strong evidence" that they were being surveilled: they were customers of Verizon Wireless and the government

163. Jewel v. NSA, ELEC. FRONTIER FOUND., https://www.eff.org/cases/jewel (last visited June 6, 2016).

164. Oral Argument at 5:55, Jewel v. NSA, 673 F.3d 902 (9th Cir. 2011) (No. 10-15616) [*hereinafter* Oral Argument, *Jewel*].

165. *Jewel*, 673 F.3d at 906.

166. *Id.* at 908. The government did not support the district court's standing analysis either: it did not discuss standing in its appellate briefs. Oral Argument, *Jewel*, *supra* note 164, at 10:18 ("We don't believe there's any question as to standing here. As [the plaintiffs' lawyer] argues, every single plaintiff has suffered an individual injury by being wiretapped.").

167. *Jewel*, 673 F.3d at 909.

168. *Id.* at 910.

169. *Id. See* Declaration of Mark Klein in Support of Plaintiffs' Motion for Preliminary Injunction at 2–7, Hepting v. NSA, No. C-06-0672 (N.D. Cal. Jun. 8, 2006).

170. *Jewel*, 673 F.3d at 910.

171. Klayman v. Obama, 957 F. Supp. 2d 1, 7 (D.D.C. 2013), *rev'd*, 800 F.3d 559 (D.C. Cir. 2015).

had unsealed court orders under which Verizon has released and continues to release call records and metadata to the government.[172] On appeal, the government has argued that the plaintiffs actually lack standing because only certain Verizon companies were required to turn over call records.[173]

III. EO 12,333 AND JUDICIAL REVIEW

In a hearing before the House Intelligence Committee on potential FISA reform, Chairman Mike Rogers argued that the fact the government had received no complaints about privacy violations in the ten years that warrantless surveillance programs had been in place suggested that the programs had not violated anyone's privacy.[174] When Stephen Vladeck pointed out that the dearth of complaints was due to the fact that the public did not know the programs existed, Rogers asserted boldly that the public's lack of awareness was precisely the reason that there had been no privacy violation.[175] In Rogers's own Orwellian words, "you can't have your privacy violated if you don't know your privacy is violated."[176]

But even someone who is oblivious to the neighbors spying on him through his bedroom window, the hacker reading his personal email, or the NSA analysts listening to his phone conversations has arguably had his privacy violated. And the Supreme Court's newfound commitment to requiring concrete and particularized injuries of the "certainly impending" variety telegraph a sinister sequel to Rogers's largely unpublicized gaffe: that if you cannot prove with *absolute certainty* that your privacy has been violated, then your privacy hasn't been violated.

The clandestine nature of the programs that the Order has been used to authorize makes proving a privacy violation even more difficult. The

172. *Id.* at 26.

173. Oral Argument at 2:45, Obama v. Klayman, 800 F.3d 559 (D.C. Cir. 2015) (No. cv-14-5004) [hereinafter Oral Argument, *Klayman*]; Yost, *supra* note 84. The government attempted to imply that the plaintiffs may not have been targeted, as the FISA Court order required Verizon Business Network Services to turn over metadata and the plaintiffs were Verizon Wireless customers. *Klayman*, 957 F. Supp. 2d at 26–27. The district court dismissed this idea as "straining mightily," especially since the government's own pleadings describe the metadata collection program as "a program that can function *only* because it 'creates a historical repository . . . *across multiple telecommunications networks*.'" *Id.* at 37 (emphasis in original). Essentially, the government was asserting that it had acted "in good faith" to create a comprehensive database to serve as an indispensable tool in fighting terrorism, while also arguing that it totally omitted Verizon Wireless customers from the dragnet. *Id.* at 38.

174. *NSA Surveillance: Mike Rogers' View of Privacy*, (C-Span3 television broadcast Oct. 29, 2013), http://www.c-span.org/video/?c4470916/mike-rogers-view-privacy.

175. *Id.*

176. *Id.* Professor Vladeck's response was that "If a tree falls in a forest, it makes a sound even if nobody's there to hear it."

communications of untold numbers[177] of U.S. persons have been swept up in the dragnet without their knowledge. That certainly does not mean that their privacy interests have not been violated but it does mean that a court, following *Clapper*, would likely find that they lack the knowledge necessary to challenge the constitutionality of the surveillance program that has potentially violated their privacy.

A. CHALLENGING EO 12,333: THE INJURY IN FACT DILEMMA

Public knowledge about the intelligence community's internal interpretations and implementations of EO 12,333 authority is incomplete. This section illustrates the difficulties that plaintiffs seeking to challenge EO 12,333 surveillance face in the post-*Clapper* landscape, as the recent case of *Schuchardt v. Obama* will illustrate.[178]

1. Injury in Fact in Post-*Clapper* Surveillance Challenges

The *Clapper* decision leaves open few possible avenues to establishing standing in a constitutional challenge to government surveillance: a past injury, such as a privacy violation or damages incurred because of past proven surveillance; a present injury, such as a present privacy violation or damages being incurred because of ongoing proven surveillance; and a future injury, such as a certainly impending privacy violation or damages incurred in preventing certainly impending future surveillance.

In the most obvious and easy case, a plaintiff who could demonstrate that the government had already intercepted his communications using the authority or program being challenged in court could likely establish an injury in fact.[179] For example, the *Jewel* plaintiffs established standing by showing that AT&T had routed all of their San Francisco customers' Internet traffic to an NSA server, which is the precise action they were

177. *Cf.* Alvaro Bedoya, *Executive Order 12333 and the Golden Number*, JUST SECURITY (Oct. 9, 2014, 10:14 AM), http://justsecurity.org/16157/executive-order-12333-golden-number/ (arguing that the exact number of Americans whose communications are "caught up in 12333 collection" is important for both policy and informed democracy).

178. Schuchardt v. Obama, No. 14-705 (W.D. Pa. 2015).

179. Judges disagree as to whether the plaintiffs need to show at the standing stage that the government's interception of their data posed an actual injury. The *ACLU* court found that the question of what constitutes an actual injury goes to the merits of a substantive Fourth Amendment claim and is therefore not relevant for standing. ACLU v. Clapper, 959 F. Supp. 2d 724, 738 (S.D.N.Y. 2013) (citing Amidax Trading Grp. v. S.W.I.F.T. SCRL, 671 F.3d 140, 147 (2d Cir. 2011)). In oral argument for *Klayman* before the D.C. Circuit, however, the panel spent a substantial amount of time querying whether simple collection could suffice as an injury. Oral Argument, *Klayman*, *supra* note 173, at 23:20. The scope of this Note does not reach this issue.

challenging.[180] And, as noted by the Court in *Clapper*, a person who received notice that their communications had been collected pursuant to a FISA surveillance directive would likely be able to establish standing to challenge the constitutionality of that directive, if not FISA itself.[181]

For a multitude of reasons, however, this route is not viable or realistic for all but a very small handful of surveillance plaintiffs. First, the government does not release the identities of its targets, much less the identities of the persons whose communications were incidentally collected. Second, in many cases, incidentally collected communications simply sit on massive NSA servers, waiting to be accessed by analysts at the touch of a key and the government has never disclosed the extent to which it collects these communications.[182] Third, although the government certainly has the ability to determine whether particular surveillance plaintiffs have actually had their communications collected, it will always assert the state secrets privilege—as it has in virtually every previous surveillance case—to avoid disclosing this information.[183]

Clapper has not completely closed the door on plaintiffs seeking to establish preventive-measure surveillance injuries. Though the majority did

180. *See* discussion *supra* Part I.B.2.

181. Clapper v. Amnesty Int'l U.S.A., 133 S. Ct. 1138, 1154 (2013).

182. CITIZENFOUR, *supra* note 5. In an interview with Laura Poitras, Edward Snowden attested to having a special level of security clearance because of his role as a systems administrator. *Id.* Snowden was not an intelligence analyst; it was not his job to "select" targets or search for possible foreign intelligence in existing NSA databases. *Id.* However, he and everyone with similar security clearances had blanket access to every database and the capability to search for any person's name within the database without supervisory approval or oversight. *Id.* The system would then return all of that person's communications—emails, instant messages. *Id.* He could also flag a person by name, email address, or other identifier, such that the system would notify him if it collected new communications associated with that person. *Id.*

183. *See, e.g.*, Jewel v. NSA, 673 F.3d 902, 913 (9th Cir. 2011) (remanding to the trial court to decide how to rule on the government's assertion of state secrets privilege); Al-Haramain v. Bush, 507 F.3d 1190, 1193–95 (9th Cir. 2007) (holding that state secrets privilege did not prevent the suit itself, but did block the admission of a document that could establish that the plaintiff was the subject of government surveillance, *even though* this document had already been inadvertently disclosed in discovery); ACLU v. NSA, 438 F. Supp. 2d 754, 758–59 (E.D. Mich. 2006) (dismissing plaintiffs' data mining claim based on government defendants' assertion of state secrets privilege); Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 980–90 (N.D. Cal. 2006) (analyzing and dismissing the government's claim of state secrets privilege); Oral Argument, *Clapper*, *supra* note 157, at 6–7 (responding to Justice Ginsburg's question as to whether the government would seek to assert the state secrets privilege if the Court were to confer standing on the *Clapper* plaintiffs, Solicitor General Verrilli said that was likely). For a more detailed discussion of the state secrets privilege and its effect on standing in government surveillance cases, see Michael C. Miller, *Standing in the Wake of the Terrorist Surveillance Program: A Modified Standard for Challenges to Secret Government Surveillance*, 60 RUTGERS L. REV. 1039, 1058–61 (2008) and *The State Secrets Privilege*, ELEC. FRONTIER FOUND., https://www.eff.org/nsa-spying/state-secrets-privilege (last visited June 6, 2016).

not explain "certainly impending" in depth, it left open the possibility that the "certainly impending" standard would allow for a plaintiff's reasonable costs to mitigate or avoid a "substantial risk" of harm to count as injury in fact. For instance, it may have reasoned that the *Clapper* plaintiffs' *particular* "attenuated" theory of injury failed to satisfy either the "certainly impending" or "substantial risk" standards.[184] Thus, a plaintiff could potentially establish standing if he knew of a substantial risk that his communications would be intercepted and undertook reasonable measures to prevent that from happening.

However, the *Clapper* plaintiffs routinely used electronic methods to communicate with the families of Guantanamo detainees and people with knowledge of terrorist activities.[185] As pointed out by the dissent, these plaintiffs were at a demonstrable risk of having their communications intercepted by Section 702, which governs the collection of electronic foreign communications. The information being exchanged between the plaintiffs and their contacts clearly had foreign intelligence value, and thus the plaintiffs had ample reason to believe that the government would use Section 702 to target their conversations and implemented reasonable preventive measures accordingly.[186] If these plaintiffs—respected and established human rights organizations and attorneys—could only establish an "attenuated" theory of injury based on those facts, then the "substantial risk" threshold must be approaching a "literally certain" risk.[187]

It is difficult to imagine, short of proof that plaintiffs were all but guaranteed to have their communications collected by the intelligence community—for example, if the government, in a fit of pique, publicly released a watch list and the plaintiffs found their names on the list—what the *Clapper* majority would consider a "certainly impending," "substantial risk." The majority provided no guidance in that regard, other than to point out the FISA notice requirement. One law professor noted that, given the hurdles that challengers to the telephony metadata program have faced, that "it is possible, however unsettling it may be, that *no one* has standing to challenge the NSA surveillance program, and thus the federal courts do not have power to consider such claims."[188]

184. *Clapper*, 133 S. Ct. at 1150 n.5. While the Court did not decide whether the "certainly impending" standard was distinct from "substantial risk," it noted in this footnote that the plaintiffs failed both here. *Id.*

185. *Id.* at 1158 (Breyer, J., dissenting).

186. *Id.*

187. *See id.* at 1150 n.5.

188. Cyrus Farivar, *If the Supreme Court Tackles the NSA in 2015, It'll Be One of These Five Cases*, ARS TECHNICA (Jan. 1, 2015, 7:00 AM), http://arstechnica.com/tech-policy/2015/01/if-the-

2. Challenging EO 12,333

An apt illustration of the difficulties that prospective plaintiffs face in challenging EO 12,333 surveillance is *Schuchardt v. Obama*, a class-action lawsuit filed in June 2014 by attorney Elliott Schuchardt attacking the constitutionality of the Order.[189] Schuchardt, like virtually every other private citizen, has limited access to information about various implementations of EO 12,333 authority. What official documents are available are often heavily redacted and many leaked documents remain unverified.[190] Assuming that the government will assert the state secrets privilege in response to Schuchardt's case as it has in virtually every surveillance case thus far,[191] this places an enormous burden on Schuchardt at the standing stage.

Schuchardt faces two main obstacles in alleging an injury in fact. First, per the majority in *Clapper*, he must show that government interception of his communications has either already occurred or is certainly impending.[192] To do this, he must show both that the surveillance programs he alleges have collected his information actually exist, and that the government actually, or at least substantially, collects "*all content*"[193]

supreme-court-tackles-the-nsa-in-2015-itll-be-one-of-these-five-cases/ (emphasis added).

189. Schuchardt v. Obama, No. 14-705 (W.D. Pa. 2015); Cyrus Farivar, *Lone Lawyer Sues Obama, Alleging Illegality of Surveillance Programs*, ARS TECHNICA (Oct. 23, 2014, 7:15 AM), http://arstechnica.com/tech-policy/2014/10/lone-lawyer-sues-obama-alleging-illegality-of-surveillance-programs/.

190. *See, e.g.*, SIGNALS INTELLIGENCE DIRECTORATE, SID MANAGEMENT DIRECTIVE NUMBER 432: PROCEDURAL GUIDELINES FOR SIGINT PRODUCTION ON U.S. [REDACTED] FIELD EXERCISES (2010), https://www.aclu.org/foia-document/signals-intelligence-directorate-sid-management-directive-432-procedural-guidelines. The redacted information includes: (1) under the "Purpose" section, the exact activity to which these particular guidelines apply, and the final purpose of the surveillance guidelines; (2) the entire "Background" section, except for the statement that certain redacted exercises provide windows of opportunity for unique SIGINT production; (3) under the "Policy Guidance and Procedures" section, a paragraph that presumably addresses the dissemination of identities of U.S. persons; (4) four categories of "Information Needs"; (5) half the "Request Procedures and Schedule for Collection" table; and (6) the subsection on "Host Nation Signals." *Id.* A host nation is any country in which U.S. SIGINT is being conducted. *Id. See also* Memorandum from Gen. Counsel to Inspector Gen. of the NSA (Mar. 31, 2009), https://www.aclu.org/foia-document/ogc-memorandum-concerning-use-material-derived-sigint (redacting parts that would explain a particular non-official use of gathered information that is apparently barred by EO 12,333 as well as two entire paragraphs, the subject of which are unknown).

191. *See, e.g.*, Jewel v. NSA, 673 F.3d 902, 905 (9th Cir. 2011); Al-Haramain v. Bush, 507 F.3d 1190, 1193–95 (9th Cir. 2007); ACLU v. NSA, 438 F. Supp. 2d 754, 758–59 (E.D. Mich. 2006); Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 980–90 (N.D. Cal. 2006); Oral Argument, *Clapper*, *supra* note 157, at 6–7.

192. *Clapper*, 133 S. Ct. at 1141.

193. Second Amended Complaint at 9, Schuchardt v. Obama, No. 14-705 (W.D. Pa. Nov. 24, 2014) [hereinafter Second Amended Complaint] (emphasis in original). Schuchardt placed great

from those services.[194] Second, because Schuchardt is challenging the constitutionality of EO 12,333, he must show that the government authorized these alleged collections under the auspices of the Order.[195]

In his pleadings, Schuchardt attempted to use an exhaustive factual overview of all the disclosures that have been made to date about post-9/11 NSA surveillance to support his claim of injury in fact.[196] The few facts relevant to his assertion of injury in fact are as follows. First, he claims to be a "consumer of various types of electronic communication" including Google, Dropbox, Facebook, Microsoft, and Verizon.[197] Citing leaked documents and interviews with whistleblowers, Schuchardt alleged that the government is collecting "all" of the data from those services: telephony metadata from Verizon and cloud data from Google, Dropbox, Facebook, and Microsoft.[198] Therefore, by logical inference, Schuchardt concluded that the government has collected all of his private email communications, search history, instant messages, and various confidential communications with his clients on those services.[199]

Schuchardt's first challenge is that he must prove that PRISM, Upstream, and any other NSA programs that allegedly collect communications and data in their entirety from Google, Facebook, and Yahoo actually exist. Proving this fact is part and parcel of alleging a concrete injury—if Schuchardt cannot demonstrate that the government is

emphasis on his assertion that the NSA has amassed all of the content from cloud services like Google and Dropbox. *See, e.g.*, *id.* at 8. If the government in fact collects 100 percent of the data from these services, then Schuchardt, by virtue of being a consumer of those services, has had his data collected. Under these circumstances, Schuchardt would have a much stronger claim for injury in fact than if the NSA selectively targeted specific people, like in *Clapper*.

194. Brief in Support of Defendants' Motion to Dismiss Plaintiffs' First Amended Complaint at 5–8, Schuchardt v. Obama, No. 14-705 (W.D. Pa. Oct. 20, 2014) [hereinafter Schuchardt Brief] (quoting Ashcroft v. Iqbal, 556 U.S. 662 (2009)). The plaintiffs made a similar argument in *Halkin v. Helms*, a 1982 D.C. Circuit case that turned on whether Vietnam War protestors had standing to seek an injunction against CIA and NSA surveillance, and to challenge the constitutionality of Executive Order 12,036, EO 12,333's predecessor. Halkin v. Helms, 690 F.2d 977, 983–84, 1001 (D.C. Cir. 1982). The plaintiffs knew of the CIA's practice of submitting names to NSA watch lists. The NSA would then scan signals transmissions and flag messages containing those names. The D.C. Circuit rejected the claims, finding that the plaintiffs could not show standing because they had alleged a generalized grievance. *Id.* at 1001–02.

195. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1151 (2013) (denying standing to challenge the constitutionality of FISA Section 702 in part because plaintiffs could not establish that their communications had been intercepted under Section 702 authority).

196. Second Amended Complaint, *supra* note 193, at 2–16.

197. *Id.* at 16. These are all companies from which the NSA has collected data wholesale via programs like PRISM. *Id.*

198. *Id.* at 7–11.

199. *Id.* at 19–20.

collecting information from certain cloud services, then he cannot demonstrate that the government collected *his* information from those cloud services. At least for the district court in *Klayman*, the confluence of confirmed government collection of all the information from a specific service provider and the plaintiff being a customer of that provider was sufficient for injury in fact.[200] In *Klayman*, however, the plaintiffs could point to official court orders unsealed by the government explicitly directing Verizon to turn over telephony metadata.[201] In *Schuchardt* on the other hand, the documents that describe the reach of the PRISM, MUSCULAR, MYSTIC, and Upstream programs were never officially verified,[202] and the government is likely to invoke the state secrets privilege to avoid having to confirm or deny their authenticity in open court.[203] Schuchardt would at most have evidence of *alleged* government collection of all the information from a specific service provider, which likely would not be enough for the case to move forward.[204]

Secondly, for Schuchardt to have suffered an "actual or imminent" or "certainly impending" surveillance injury, he will likely need to show that the alleged programs collect all, or at least a substantial amount of, data from every consumer of Google, Facebook, and Yahoo. Without establishing that the government collected a significant amount of, if not all, the content from the listed services, he would not be able to establish with a high degree of certainty that the government had collected *his* content. Consider the fact that the *Clapper* court denied standing to the plaintiffs even though they could show that they routinely engaged in electronic communications with non-U.S. persons that were substantially relevant to national security, the anti-terrorism effort, and foreign intelligence. If Schuchardt could show that the alleged programs were real and that they collected all of the information from his service providers, his case for injury in fact would be more analogous to that of the *Klayman* plaintiffs. However, the government is highly unlikely to officially release information about the content collection programs with any specificity.

200. Klayman v. Obama, 957 F. Supp. 2d 1, 9 (D.D.C. 2013), *rev'd*, 800 F.3d 559 (D.C. Cir. 2015).

201. *Id.*

202. James Clapper acknowledged that the programs existed in some form, but insisted they were inaccurately described. *See* Press Release, Clapper, *supra* note 7. Thus, many of the details of PRISM remain unconfirmed.

203. *See, e.g.*, sources cited *supra* note 183.

204. Standing issues aside, the government is likely to invoke the state secrets privilege on the grounds that "information necessary to litigate plaintiffs' claims" (i.e., detailed information about alleged content-scraping surveillance programs) is protected from disclosure by the privilege. *See, e.g.*, Jewel v. NSA, 673 F.3d 902, 906 (9th Cir. 2011).

These programs are arguably more controversial than the telephony metadata program, which does not collect the substantive content of any communications.

Finally, as EO 12,333 is the subject of Schuchardt's challenge, he must show that his communications were collected pursuant to EO 12,333 authority.[205] To do so, he cites President Obama's Signals Intelligence Presidential Policy Directive ("PPD-28")[206] and John Tye's exposé.[207] Neither of these arguments is likely to succeed. First, while PPD-28 laid out the Obama administration's signals intelligence goals and general policy, it only mentions the Order in passing, to incorporate the definitions of certain terms, such as "intelligence" and "U.S. persons," by reference.[208] It also mentions the Order once as a frame of reference for establishing limits on the dissemination of certain information.[209] At no point does it say that any surveillance has been authorized pursuant to *any* specific executive order. Second, while Tye's op-ed and interview statements were all pre-approved by the NSA and the State Department, a court would be unlikely to find this sufficient to establish that the Order was actually used to authorize the actions being challenged by Schuchardt.[210] The government could easily argue that the NSA required pre-clearance only to assure that Tye did not reveal any classified information, not because he was acting as a spokesperson for the government.[211] While documents like U.S. Signals Intelligence Directive 18[212] and DOD 5240.1-R show that the Order is used to authorize *some* surveillance,[213] a court would likely require some official, specific substantiation of Schuchardt's allegations. Otherwise, Schuchardt will not be able to identify a specific government action that can be challenged. In turn, the government would most likely assert the state secrets privilege to keep the information from coming into the record.[214]

205. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148–49 (2013) (holding that the challenged government surveillance must be fairly traceable to FISA if the plaintiffs wanted to challenge FISA's constitutionality).

206. *See generally* ADMIN. OF BARACK OBAMA, DIRECTIVE ON SIGNALS INTELLIGENCE ACTIVITIES: PRESIDENTIAL POLICY DIRECTIVE/PPD-28 (2014), http://www.gpo.gov/fdsys/pkg/DCPD-201400031/pdf/DCPD-201400031.pdf [hereinafter PPD-28].

207. Second Amended Complaint, *supra* note 193, at 12–14.

208. PPD-28, *supra* note 206, at 1–5.

209. *Id.* at 5.

210. PCLOB Public Meeting Transcript, *supra* note 16, at 71 (statement of John Tye).

211. *Id.*

212. NAT'L SEC'Y AGENCY, *supra* note 24, at 2.

213. *See* discussion *supra* Part I.B.2.

214. *See, e.g.*, sources cited *supra* note 183.

Thus, Schuchardt finds himself in a familiar bind: despite the fact that public knowledge of post-9/11 government surveillance is greater than ever, he lacks the resources and ability to allege facts with enough specificity to be able to challenge EO 12,333 in court. The biggest problem is the clandestine nature of existing EO 12,333 surveillance programs, which is unlikely to change given the government's understandable—and likely justifiable—reluctance to release information that could compromise valuable intelligence-gathering programs. However, as EO 12,333 itself states, these activities must comply with the Fourth Amendment and the Constitution, and American citizens who believe that their privacy interests have been violated without sufficient legal justification should have a fair chance to challenge alleged violations in court.

B. NEW APPROACHES

Commentators have proposed a variety of solutions to the troubling standing quandary posed by secret government surveillance programs. The possibilities include developing alternative conceptions of injury in fact, recognizing a new category of privacy harms,[215] adopting a statutory injury approach that allows the legislature to define the required injury in fact for challenging certain laws,[216] and streamlining the varying approaches to probabilistic injuries in standing doctrine by adopting a new, consistent standard.[217]

For instance, commentators have argued in favor of adopting the "objectively reasonable likelihood" standard used by the Second Circuit in the *Clapper* case,[218] as well as the "reasonable fear of harm from undisputed conduct standard"[219] fashioned in *Friends of the Earth v. Laidlaw*.[220] An objective reasonableness standard would preserve the integrity of standing doctrine and respect major justiciability concerns. Additionally, a reasonable likelihood standard is not so stringent as to prevent legitimate plaintiffs from being able to challenge dragnet

215. Scott Michelman, *Who Can Sue Over Government Surveillance?*, 57 UCLA L. REV. 71, 75 (2009). *But see* Cassandra Barnum, Comment, *Injury in Fact, Then and Now (And Never Again):* Summers v. Earth Island Institute *and the Need for Change in Environmental Standing Law*, 17 MO. ENVTL. L. & POL'Y REV. 1, 7–25 (2009) (arguing that the injury in fact requirement has no basis in either constitutional or prudential separation-of-powers justifications for standing, and should be eliminated entirely).

216. Rubow, *supra* note 131, at 1023–24 (adopting the "statutory violation as standing" standard of Edwards v. First Am. Fin. Corp., 610 F.3d 514 (9th Cir. 2010)).

217. *See* discussion *supra* Part I.B.1.

218. Michelman, *supra* note 215, at 113.

219. Miller, *supra* note 183, at 1070.

220. Friends of the Earth, Inc. v. Laidlaw Envtl. Servs., Inc., 528 U.S. 167, 184 (2000).

surveillance in court. Recall *Monsanto*, in which the Court saw fit to allow standing based in part on an assertion of a "reasonable likelihood" of harm.[221]

However, absent a massive shift in government surveillance law or significant personnel change on the Court, it seems highly unlikely that *Clapper* will be overruled in the near future, which reconceptualizing injury in fact in surveillance cases would likely require. *Clapper*, after all, stands for the proposition that surveillance plaintiffs must show that any probabilistic privacy violations are "certainly impending." However, the Court has generally displayed extreme reluctance to overturning its recent decisions.[222] When it has done so, many have suspected that personnel changes and shifts in political preferences have been responsible.[223] For example, in 2010, the Court's controversial *Citizens United v. FEC*[224] decision overruled *Austin v. Michigan Chamber of Commerce*, decided in 1990, and *McConnell v. FEC*, decided only seven years prior in 2003,[225] sparking outrage and accusations that the decision was solely due to shifts in Court composition.[226]

221. *See* discussion *supra* Part I.B.1.

222. *See* CONG. RESEARCH SERV., THE CONSTITUTION OF THE UNITED STATES OF AMERICA: ANALYSIS AND INTERPRETATION 2387–99 (Johnny H. Killian et al. eds., 2004) (listing every Supreme Court case explicitly overruling a prior decision). The Supreme Court has expressly overruled itself only twice in the past six years. The first overruling was *Citizens United v. FEC*, 558 U.S. 310 (2010), discussed below. The second was *McDonald v. City of Chicago*, 561 U.S. 742 (2010), which overruled some much older cases.

223. Payne v. Tennessee, 501 U.S. 808, 844 (1991) (Marshall, J., dissenting) ("Neither the law nor the facts supporting *Booth* and *Gaithers* underwent any change in the last four years. Only the personnel of this Court did."). *See, e.g.*, GEORGE COSTELLO, THE SUPREME COURT'S OVERRULING OF CONSTITUTIONAL PRECEDENT: AN OVERVIEW 2–3 (2005) (pointing out that the justices overrule precedents for a variety of competing reasons, among them policy preferences, and that it is difficult to predict whether a decision will be overruled); James F. Spriggs, II & Thomas G. Hansford, *Explaining the Overruling of U.S. Supreme Court Precedent*, 63 J. POL. 1091, 1093–94 (2001) (arguing that Supreme Court justices are motivated to overrule past decisions by their policy preferences, though tend to work within doctrinal constraints).

224. *Citizens United*, 558 U.S. at 311–12 (explicitly overruling *Austin v. Michigan Chamber of Commerce*, 494 U.S. 652 (1990) and *McConnell v. FEC*, 540 U.S. 93 (2003), finding that the government cannot limit corporate spending on political speech).

225. *Austin*, 494 U.S. at 659–660 (finding that the government has a compelling interest in preventing the "corrosive and distorting effects" of corporate spending on political speech); *McConnell*, 540 U.S. at 94–95 (2003) (upholding a statute that prohibited corporations from using general treasury funds to influence federal elections).

226. *See, e.g.*, Michael S. Kang, *After* Citizens United, 44 IND. L. REV. 243, 248–49 (2010) (stating that while the Rehnquist Court was highly deferential to the government in campaign finance cases, the Roberts Court had by 2010 already struck down a number of campaign finance regulations, with the only differences in circumstances being the replacement of Chief Justice Rehnquist and Justice O'Connor with Chief Justice Roberts and Justice Alito).

Thus, given the Supreme Court's reluctance to overrule past decisions, it could, in a subsequent case, distinguish *Clapper* to allow standing to plaintiffs seeking to challenge secret government surveillance, just as the *Clapper* majority conveniently disregarded the *Monsanto* litigants' "reasonable likelihood" of harm and preventive-measure injuries.[227]

1. Distinguishing *Clapper*

In a future challenge to secret government surveillance authorized pursuant to EO 12,333, future courts can distinguish, or "narrow,"[228] *Clapper* for several reasons. First, FISA Section 702, which was at issue in *Clapper*, provides for built-in, procedurally required judicial review. EO 12,333 does not. Second, the notice requirement in FISA Section 702 provides an opportunity for targets of FISA surveillance to prove that they have suffered an actual privacy violation if they want to contest the constitutionality of that surveillance. Targets of EO 12,333 surveillance do not have even that.

One way for future courts to distinguish *Clapper* would be to point out the two major differences between FISA Section 702 and EO 12,333: the existence of built-in, procedurally required judicial review and notification requirements. Even if the FISA Court has minimal latitude in deciding whether to authorize a particular surveillance directive, it still has the opportunity to review the government's procedures with an eye to whether they comport with the Fourth Amendment.[229] EO 12,333 surveillance programs and procedures, on the other hand, need only be approved by the heads of individual intelligence community elements, the Attorney General, and the DNI.[230] The procedures do not undergo mandatory judicial, or even congressional, review. While some surveillance procedures are ultimately revealed to Congress, the information is only made available on a need-to-know, high security clearance basis.[231] Although some members of Congress have the requisite security clearances to review the procedures, their staff—who actually read and screen the

227. *See* discussion *supra* Parts I.B.2, II.A.

228. *See* Richard M. Re, *Narrowing Precedent in the Supreme Court*, 114 COLUM. L. REV. 1861, 1865–66 (2014).

229. *See* discussion *supra* Part I.A.1.

230. EO 12,333, *supra* note 13, at §§ 1.5(r), 1.6(a), 2.5.

231. *See* Letter from Senator Ron Wyden & Senator Mark Udall to Attorney Gen. Eric Holder, United States Senate (Mar. 15, 2012), https://www.documentcloud.org/documents/325953-85512347-senators-ron-wyden-mark-udall-letter-to.html (expressing concerns about the secrecy of legal interpretations of public government authorities).

documents that members of Congress receive—do not.[232] Thus, members of Congress do not, as a practical matter, regularly review this information.[233] Given this lack of oversight, it seems even more important that Americans who have concerns about the widespread nature and secrecy of government dragnet surveillance have the opportunity to challenge the programs in court.

The *Clapper* majority understandably attributed some importance to the notification requirement.[234] If it were routinely and transparently used,[235] each person who received notice would know, with certainty, that the government had collected his or her communications under FISA Section 702. Armed with that information, those people could, if they so wished, challenge either the directive or Section 702 itself in court. Even though this would likely only apply to a very small fraction of people that the government has targeted using FISA Section 702, the number is still greater than zero. FISA is not functionally foreclosed from judicial review. On the other hand, a person who has been targeted under an EO 12,333 program would never have the opportunity to find out about the surveillance. Even if he or she was subsequently prosecuted based on information the government obtained through an EO 12,333 program, the DOJ has no legal obligation to inform him or her of the source of their information prior to the proceeding. And what of the unknown number of Americans whose private information is readily available to NSA intelligence analysts at their discretion? Dragnet surveillance by nature sweeps in communications of countless innocent people.

A future court could conclude that the Order's lack of basic protections and safeguards raise implicit fairness concerns that are simply too high value to apply the rigid and unforgiving "certainly impending" standard conceptualized by the *Clapper* majority.[236] Recall that the *Clapper* majority specifically addressed the concern that FISA Section 702 was insulated from judicial review and argued that this was not so for three distinct reasons: targeting and minimization procedures are evaluated to see if they comport with the Fourth Amendment at the outset, the notice requirement opens an avenue to establish standing, and electronic communications providers can challenge FISA directives to the FISA

232. *Id.*

233. *Id.*

234. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1154–55 (2013).

235. The DOJ arguably has not adhered to the FISA notice requirement. *See supra* note 159 and accompanying text.

236. *Clapper*, 113 S. Ct. at 1147–50.

Court.[237] The Order does not provide for any of those protections. If those were the only three reasons that *Clapper*'s high threshold for surveillance harms did not insulate a particular surveillance authority from judicial review, and none of them are applicable to the Order, then it follows that there is a substantial possibility that *Clapper*'s standard insulates the Order from judicial review.

A future court could find that this foreclosure is improper, and distinguish *Clapper* on this basis. It could agree with the *Clapper* majority that surveillance plaintiffs must allege a "substantial risk"[238] that the government will intercept their communications but exercise discretion in determining what constitutes a substantial risk. For example, the *Monsanto* farmers alleged a reasonable risk of cross-contamination with their organic alfalfa crops by demonstrating physical proximity to genetically modified crops.[239] A court could similarly find, for example, that Elliott Schuchardt could allege a substantial risk that the government intercepted his privileged and confidential communications and emails by demonstrating that the government collects a substantial amount of communications and emails from those service providers.

CONCLUSION

The United States intelligence community has used EO 12,333 to authorize surveillance programs that provide for the acquisition and retention of a significant amount of information pertaining to U.S. persons. The Order does not contain any provision that would require an element of the intelligence community to notify either surveillance targets or persons whose communications were incidentally collected.[240] Any American's email communications could be sitting in an NSA database, waiting to be read, and the government would have no duty or obligation under any circumstance to notify that person. For that reason, and the secrecy issues discussed above, EO 12,333 surveillance is effectively insulated from judicial review.

Given the extent of public backlash to these revelations, coupled with the fact that scattered federal district courts that have ruled on the constitutionality of the secret surveillance programs have found them to be unconstitutional, a future court could open an avenue for surveillance

237. *Id*. at 1154–55.
238. *Id.* at 1150 n.5.
239. Monsanto Co. v. Geertson Seed Farms, 51 U.S. 139, 153–55 (2009).
240. *But see* 50 U.S.C. §§ 1806(c), 1881a (2012).

plaintiffs to establish standing by distinguishing *Clapper*. It need not overrule the "certainly impending" requirement—it need only clarify that the plaintiffs must demonstrate a substantial risk that their communications have been or will be intercepted and apply the standard less stringently than the *Clapper* majority. Otherwise, the recent spate of EO 12,333 disclosures from whistleblowers and leakers alike will be the low-hanging fruit branches and receding water to the American public's Tantalus—we can clearly see that our privacy has been violated, but have no way of touching it.