Standing and Covert Surveillance

Christopher Slobogin*

Abstract

This Article describes and analyzes standing doctrine as it applies to covert government surveillance, focusing on practices thought to be conducted by the National Security Agency. Primarily because of its desire to avoid judicial incursions into the political process, the Supreme Court has construed its standing doctrine in a way that makes challenges to covert surveillance very difficult. Properly understood, however, such challenges do not call for judicial trenching on the power of the legislative and executive branches. Instead, they ask the courts to ensure that the political branches function properly. This political process theory of standing can rejuvenate the "chilling" arguments that the Supreme Court has rejected in Fourth and First Amendment cases. Additionally, the theory provides a third, independent cause of action against covert surveillance that is based on separation of powers principles, specifically the notion that, in a representative democracy governed by administrative law principles, one role of the courts is to ensure that the legislative branch authorizes and monitors significant executive actions and that the executive branch promulgates reasonable regulations governing itself. Litigants who can show that their participation in the political process has been concretely compromised by covert surveillance should have standing to bring any of these causes of action.

* Milton Underwood Professor of Law, Vanderbilt University Law School. The author would like to thank participants at the National Security Symposium held at Pepperdine University School of Law on April 4, 2014, and participants at a workshop at Vanderbilt Law School for their comments on this Article.

I. INTRODUCTION

By all reports, covert government surveillance activities—surveillance programs meant to be kept secret from the general public—have expanded tremendously in scope since September 11, 2001.[1] Because much of this surveillance is conducted without a warrant or probable cause, it may violate the Fourth Amendment or some other constitutional provision.[2] But to make that argument in court a litigant must have standing, which according to the Supreme Court exists only when the challenger can make a plausible claim of "injury" that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[3] Precisely because much modern-day surveillance is covert, this demanding standing test may be impossible to meet.[4] If so, unconstitutional surveillance programs may be immune from judicial review.[5]

This Article describes and analyzes standing doctrine as it applies to covert government surveillance, focusing primarily on practices thought to be conducted by the National Security Agency (NSA), although the analysis

1. *See infra* text accompanying notes 9–16.

2. *See* U.S. CONST. amend. IV; *see also* New Jersey v. T.L.O., 469 U.S. 325, 370 (1985) ("Full-scale searches unaccompanied by probable cause violate the Fourth Amendment.").

3. Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010) (citing Horne v. Flores, 557 U.S. 433, 445 (2009)); *see also* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992) (stating that, under the Court's cases, "the irreducible constitutional minimum of standing" requires the plaintiff to show: (1) "an 'injury in fact' . . . which is (a) concrete and particularized, and (b) 'actual or imminent, not "conjectural" or "hypothetical"'"; (2) "a causal connection between the injury and the conduct complained of"; and (3) a non-speculative likelihood that the injury will be "'redressed by a favorable decision'" (citations omitted)).

4. *See, e.g.*, Scott Michelman, *Who Can Sue Over Government Surveillance?*, 57 UCLA L. REV. 71, 79 (2009) ("[A]lthough there is judicial consensus that the invasion of privacy that results from being spied on is injurious, plaintiffs have difficulty establishing that they are, in fact, being spied on.").

5. *See, e.g.*, *id.* at 89–99; *see also infra* text accompanying notes 21–35.

could also apply to covert domestic surveillance programs, such as fusion centers.[6] Part II of the Article describes the current state of standing law in the covert surveillance context. The Supreme Court has made challenges to this type of surveillance very difficult, on the ground that they intrude upon the power of the legislative and executive branches. Part III of this Article explains why this view misconstrues the nature of claims that contend covert surveillance practices are unconstitutional. Whether based on the Fourth Amendment's prohibition on unreasonable searches and seizures or the First Amendment's guarantee against abridgements of speech and association, these claims seek to ensure that the political branches carry out their proper roles. Specifically, in contrast to most types of generalized claims that are routinely dismissed on standing grounds, these cases seek to ensure that the legislative branch does not grant, and the executive branch does not usurp, power that can undermine the foundations of the democratic process. Relying on the process theory of John Hart Ely, this part demonstrates why litigants who can show that their ability to participate in the political process has been compromised by covert surveillance should have standing to make these constitutional claims even if they cannot prove the surveillance has been directed at them.

Part IV of the paper anticipates a counter-argument, explicitly recognized in the Court's Fourth Amendment cases, that standing is merely another method of assessing whether the substantive threshold of the relevant constitutional provision—infringement of reasonable expectations of privacy in the Fourth Amendment context and abridgement of speech or association in the First Amendment setting—has been crossed; if that is the correct approach to standing doctrine, then, regardless of their impact on the political process, some types of covert surveillance might not be challengeable because, at least as the law stands now, they do not implicate either the Fourth or First Amendments. Relying on other work of mine, this part asserts that political process theory also provides a basis for a third

6. These centers "fuse" together information from a wide variety of computerized sources. *See* THE CONSTITUTION PROJECT, RECOMMENDATIONS FOR FUSION CENTERS: PRESERVING PRIVACY AND CIVIL LIBERTIES WHILE PROTECTING AGAINST CRIME AND TERRORISM 4–7 (2012), *available at* constitutionproject.org/pdf/fusioncenterreport.pdf. There are over 70 such centers in the country, some of them employing more than 200 people, *id.* at 7, yet they are subject to only minimal regulation. *See* Frank Pasquale & Danielle Keats Citron, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1444 (2011) (arguing that "the lack of oversight of fusion centers is both eroding civil liberties *and* wasting resources").

cause of action, based on separation of powers principles. This third cause of action asserts that, in a representative democracy governed by administrative law principles, one role of the courts is to ensure that the legislative branch authorizes and monitors significant executive actions and that the executive branch promulgates reasonable regulations governing itself. If this cause of action is recognized, any litigant whose participation in the political process is concretely affected by covert surveillance should have standing to bring it, even if the Fourth and First Amendments are dead letters in the surveillance context.

Part V of the paper briefly addresses some objections to these arguments in favor of standing, the primary one of which is that national security matters should be handled differently than other cases. In fact, as recent allegations about the effects of executive branch spying on members of Congress and the press accentuate,[7] it is precisely national security cases that most dramatically raise political process issues requiring the attention of the judiciary. These cases bring home the point that standing doctrine should be structured so that the courts have a role in ensuring the continued viability and independence of the legislative and executive branches, goals that the Court says standing doctrine is designed to enhance. As Chief Justice Roberts has said, albeit in a decision outside the standing context, "[T]he obligation of the Judiciary [is] not only to confine itself to its proper role, but to ensure that the other branches do so as well."[8]

II. THE DIFFICULTY OF OBTAINING STANDING IN COVERT SURVEILLANCE CASES

Thanks to Edward Snowden, the federal government—up to and including President Obama—has been forced to confirm that the National Security Agency is vacuuming up every phone number we text and call, and is then subjecting this "metadata" to queries to determine which numbers link with known or suspected terrorists.[9] Press reports suggest that the NSA

7. *See, e.g.*, *infra* text accompanying notes 125–26 (discussing Senator Dianne Feinstein's allegations that the CIA hacked computers used by the Senate Select Intelligence Committee).

8. City of Arlington v. FCC, 133 S. Ct. 1863, 1886 (2013) (Roberts, C.J., dissenting).

9. *See* David S. Kris, *On the Bulk Collection of Tangible Things*, LAWFARE RES. PAPER SERIES, Sept. 29, 2013, at 1, 6 & n.24, *available at* http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf (describing the government's admissions regarding the existence of the metadata collection).

is also engaging in numerous other types of "panvasive" surveillance (that is, surveillance that cuts across wide swaths of the population with no particularized reason to suspect any given subject of terrorist activity or other wrongdoing).[10] F. Michael Maloof of WND has asserted that "[t]he National Security Agency already has access to all the content of intercepted emails and phone calls, not just the 'metadata' such as who contacted who[m], when and where."[11] Glenn Greenwald, the Guardian journalist who is Snowden's main conduit to the outside world, has described XKeyscore, "[a] top secret National Security Agency program" that purportedly "allows analysts to search with no prior authorization through vast databases containing emails, online chats and the browsing histories of millions of individuals."[12] Via a program code-named "Optic Nerve," the NSA and its British counterpart reportedly have been amassing webcam images of millions of Yahoo users since at least 2008.[13] A newly disclosed malware program known as "Turbine" allegedly allows the NSA to hack into computers, computer networks, and phone networks.[14] Today Turbine affects thousands of people but it is predicted to soon to reach "millions."[15] One calculation holds that the NSA "touches" roughly half of all Internet communications and that, because 68% of those communications are spam, the agency may have access to all meaningful communication on the Internet.[16]

10. *See* Christopher Slobogin, *Rehnquist and Panvasive Searches*, 82 MISS. L.J. 307, 308 (2013) (coining the term "panvasive surveillance").

11. *See* F. Michael Maloof, *Yes, NSA Has* Content *of Phone Calls, Emails*, WND (June 10, 2013, 7:56 PM), http://www.wnd.com/2013/06/yes-nsa-has-content-of-phone-calls-emails/#tfjdBTJ0WOUps%20PZ9.%2099.

12. *See* Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet,"* GUARDIAN, July 31, 2013, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

13. *See* Amy Goodman, *Peeping Webcam? With NSA Help, British Spy Agency Intercepted Millions of Yahoo Chat Images*, DEMOCRACY NOW! (Feb. 28, 2104), http://www.democracynow.org/2014/2/28/peeping_webcam_with_nsa_help_british.

14. *See* Amy Goodman, *Snowden Docs Expose How the NSA "Infects" Millions of Computers, Impersonates Facebook Server*, DEMOCRACY NOW! (Mar. 17, 2014), http://www.democracynow.org/2014/3/17/snowden_docs_expose_how_the_nsa.

15. *See id.*

16. *See* Jeff Jarvis, *How Much Data the NSA Really Gets*, GUARDIAN, Aug. 13, 2013, http://www.theguardian.com/commentisfree/2013/aug/13/nsa-internet-traffic-surveillance.

Most of this surveillance takes place without any type of judicial authorization,[17] or is authorized only by the Foreign Intelligence Surveillance Court (FISC), which operates in secret.[18] Although regulation of these practices has recently ramped up, even today the decision about what to collect and what to target and query is largely in the hands of executive agency officials.[19] Thus, good arguments can be made that much, if not all, of this surveillance is unconstitutional under the Fourth Amendment, the First Amendment, separation of powers doctrine, or some combination thereof.[20] But these arguments may never be fully fleshed out in the courts because of the Supreme Court's standing doctrine.

The Court's recent decision in *Clapper v. Amnesty International USA*[21] involved a challenge to section 702 of the Patriot Act, which allows the NSA to intercept communications of non-U.S. persons outside the United States in the absence of individualized suspicion.[22] Despite the plaintiffs' showing that they routinely made overseas calls to parties likely to be targeted under section 702, the Court denied them standing because they could not show that their calls were in fact intercepted and thus could not prove that the injury they alleged due to the surveillance was either "actual" or "certainly impending."[23] As the outcome in *Clapper* illustrates, because NSA surveillance is, by design, covert, the standing requirement that plaintiffs allege a "concrete" injury can pose a serious obstacle to parties trying to challenge it.[24] The majority in *Clapper* nonetheless insisted that "our holding today by no means insulates [section 702] from judicial review."[25]

17. *See* Greenwald, *supra* note 12.

18. For a description of how the court works, see *Foreign Intelligence Surveillance Court (FISC)*, ELECTRONIC PRIVACY INFO. CENTER, https://epic.org/privacy/terrorism/fisa/fisc.html (last visited Nov. 19, 2014).

19. *See infra* notes 43–45, 162 and acompanying text.

20. For Fourth and First Amendment arguments, see CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 98–101, 180–96 (2007). For separation of powers arguments, see *infra* notes 140–52 and accompanying text.

21. 133 S. Ct. 1138 (2013).

22. *See* 50 U.S.C. § 1881a(a), (b) (2012) (allowing the Attorney General and the Director of National Intelligence to acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are not "United States person[s]" and "are reasonably believed to be located outside the United States").

23. *Clapper*, 133 S. Ct. at 1143 ("[R]espondents' theory of *future* injury is too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'").

24. *See also infra* notes 90–100 and accompanying text.

25. *Clapper*, 133 S. Ct. at 1154.

It noted that the Foreign Intelligence Surveillance Act requires that the government give notice when it "intends to use or disclose [any] information obtained or derived from [electronic surveillance]" in a criminal prosecution, and pointed out that, armed with such notice, the defendant could mount a challenge to section 702.[26]

Unfortunately, the Court's optimistic view of how the Foreign Intelligence Surveillance Act's notice requirement works was not accurate. First, for undetermined reasons, at the time *Clapper* was decided the Department of Justice was not providing the required notice, despite Solicitor General Donald Verilli's assertion to the contrary during oral arguments in that case.[27] Only in late 2013, apparently after prodding from Verilli, did the DOJ reverse its policy and begin following the statute; even since then, however, it is not clear that the DOJ has provided notice every time it is required to do so.[28] Moreover, through a process known as "parallel construction," the government has been known to launder its surveillance results by surreptitiously providing them to investigators who, clued-in by the covertly-obtained information, then pursue the investigation through more overt means.[29] Thus, even in connection with interceptions of

26. *Id.*

27. *See* Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. TIMES, July 15, 2013, http://www.nytimes.com/2013/07/16/us/double-secret-surveillance.html?pagewanted=all (noting cases in which federal prosecutors refused to disclose the source of their evidence, despite the high likelihood that it came from NSA surveillance).

28. *See* Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES, Oct. 16, 2013, http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html?pagewanted=all (detailing the debate between Verilli and NSA lawyers as to when a duty to disclose is required under the Patriot Act); Mike Masnick, *DOJ Flips Out That Evidence Gathered Via FISA Orders Might Be Made Available to Defendants*, TECHDIRT (Apr. 3, 2014, 1:55 PM), www.techdirt.com/articles/20140402/12194426777 ("[T]he DOJ will do *everything possible* to keep the details of what was done via FISA (and whether or not it was legal or appropriate) out of the case.").

29. *See* John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS, Aug. 5, 2013, *available at* http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805 ("A secretive U.S. Drug Enforcement Administration unit is funneling information from intelligence intercepts, wiretaps, informants and a massive database of telephone records to authorities across the nation to help them launch criminal investigations of Americans."); Mike Masnick, *Parallel Construction Revealed: How the DEA Is Trained to Launder Classified Surveillance Info*, TECHDIRT, (Feb. 3, 2014, 11:49 AM), http://www.techdirt.com/articles/20140203/11143926078/parrallel-construction-revealed-how-dea-is-trained-to-launder-classified-surveillance-info.shtml (stating, based on perusal of government training materials, that parallel construction is a "common practice" in the Drug Enforcement Administration); *see also* Ray McGovern, *How the NSA Criminally Aids Criminal Cases*,

the contents of electronic communications, standing may be hard to come by.

More importantly for present purposes, no notice requirement analogous to the provision in section 702 exists in connection with other covert surveillance programs, in particular the metadata and PRISM programs that collect phone and Internet information.[30] These programs are authorized (or at least the national security establishment says they are authorized)[31] under section 215 of the Patriot Act,[32] a separate subchapter from the communications interception subchapter that does not include a defendant-notice provision; indeed, it states just the opposite.[33] Although Section 215 does permit third party providers who possess the data to contest a government request for it,[34] these parties have little incentive to do so, at least on grounds relevant to their customers.[35] In short, after *Clapper* these

---

TRUTHOUT (June 16, 2014, 10:13 AM), http://www.truth-out.org/news/item/24379-how-nsa-can-secretly-aid-criminal-cases ("[T]he government simply perjures itself during the court discovery process by concealing the key role played by the NSA database . . . .").

30. *See* BRENNAN CENTER FOR JUST., N.Y. U. SCH. L., ARE THEY ALLOWED TO DO THAT? A BREAKDOWN OF SELECTED GOVERNMENT SURVEILLANCE PROGRAMS 3 (2013), *available at* http://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf (noting that, under the NSA's metadata and PRISM programs, "targeted persons generally have no way of knowing that their records are the subject of specific government scrutiny"). The same can be said with respect to several other metadata programs, *see* Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants and the Right to Notice*, 54 SANTA CLARA L. REV. 843, 878–95 (2015), and investigations that intercept the content of communications collected outside the United States under authority of Executive Order 12333. *See* Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights*, N.Y. TIMES, Aug. 13, 2014 (stating that government officials assert they are not required to provide notice in this setting).

31. *See, e.g.*, Brief for Defendants-Appellees at 30–41, ACLU v. Clapper, No. 14-42 (2d Cir. Apr. 10, 2014), *available at* https://www.aclu.org/sites/default/files/assets/2014-04-10_clapper_govt-opposition-brief.pdf. For counter-arguments, see Brief for Plaintiffs-Appellants at 11–17, ACLU v. Clapper, No. 14-42 (2d Cir. Apr. 24, 2014), *available at* http://pdfserver.amlaw.com/nlj/usca2-aclu-replybrief.pdf, and Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757 (2014).

32. *See* 50 U.S.C. § 1861 (2012).

33. *See id.* § 1861(d) ("No person shall disclose to any other person [other than those persons necessary to produce the tangible things under this section] that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section . . . .").

34. *See* 12 U.S.C. § 3414(a)(3)(C) (Supp. I 2013) (allowing recipient of order to consult an attorney).

35. In fact, it is unclear whether the third parties have standing in this context. *See* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 328 (2012) (noting that "[t]he provider's own privacy interests are not at stake"). Even if they have standing, the third party's interests are often diametrically opposed to the interests of the

programs are even more impervious to challenge than the intercept program challenged in that case.

Despite all of this, two lower federal courts have been willing to grant standing to civil litigants challenging the NSA's metadata program. The decision with the most detailed analysis of the standing issue is *Klayman v. Obama* (which went on to question the program's constitutionality).[36] Noting that *Clapper* was decided before Snowden's disclosures, federal district court Judge Richard Leon found that case inapposite;[37] the government's subsequent confirmation of Snowden's revelation that the NSA was going after virtually everyone's metadata, he stated, provided "strong evidence that [plaintiff's] telephony metadata has been collected."[38] To the government's assertion that, at best, this reasoning justified granting standing to challenge the bulk collection of the metadata and not the NSA's querying of specific numbers, Judge Leon responded that, in order for the query process to work, the NSA "must necessarily analyze metadata for *every* phone number in the database by comparing the foreign target number against *all* of the stored call records to determine which U.S. phones, if any, have interacted with the target number."[39]

Had he been writing on a blank slate, Judge Leon's reasoning would have been a sensible way of analyzing the standing issue raised in *Klayman*. However, when viewed through the restrictive lens of *Clapper*, his standing analysis is at best only halfway persuasive. Least unassailable is his conclusion with respect to a plaintiff's ability to contest the first-stage, bulk collection of metadata. The government itself conceded, in the course of

citizens whose information they possess. *See id.* ("Although there may well be instances in which a provider might 'push back' against law enforcement in response to particular orders, providers rarely appeal to a higher court."); Avidan Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 IOWA L. REV. (forthcoming 2015) (manuscript at 4), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2523647## (noting that corporations "cannot serve a government-checking function when powerful tech companies function almost like mini-states with vested interests in cooperating with government").

36. 957 F. Supp. 2d 1, 37–42 (D.D.C. 2013) (concluding that there was a reasonable likelihood that plaintiffs would succeed in showing that the NSA's metadata collection activities were unreasonable searches under the Fourth Amendment); *see also* ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (holding that the NSA's collection of metadata related to non-profit civil rights and liberties organizations' phone calls constituted an actual injury sufficient to give the organizations standing), *appeal docketed*, No. 14-42 (2d Cir. Jan. 2, 2014).

37. *Klayman*, 957 F. Supp. 2d at 26.

38. *Id.*

39. *Id.* at 28.

arguing for the necessity of the bulk collection, that the metadata program could only work if the NSA were allowed to develop and maintain for extended periods a repository of all communications across multiple communications networks;[40] otherwise, the government asserted, it would not be able to make the connections between numbers suspected to be terrorism-related and numbers in the United States.[41] While the government only admitted to obtaining this information from the most common communications carriers, that admission would still mean that any plaintiff who uses Verizon, AT&T, or the other big carriers could show they have been affected by the bulk collection procedure.[42]

Judge Leon's conclusion that the plaintiffs also had standing to contest the NSA's warrantless queries of collected metadata is not as airtight. According to NSA officials, at the time of the *Klayman* litigation, queries began with a "seed identifier" number or email address that one of twenty-two designated NSA officials had "reasonable, articulable suspicion" to believe was associated with a terrorist organization;[43] the agency then identified contacts up to "three hops" out from this seed identifier[44] (a procedure that was changed in significant ways by order of President Obama in January 2014).[45] As indicated above, in finding standing to contest this

40. *Id.* at 27 (noting that the Government stated in its pleadings that the bulk metadata collection program "can function *only* because it 'creates an historical repository that permits retrospective analysis of terrorist-related communications *across multiple telecommunications networks*'").

41. *Id.*

42. *See id.* Even this proof, however, does not *necessarily* mean that they have standing under the Supreme Court's cases, unless it can also be shown that the government plans to use data from the bulk collection against the plaintiffs. *See infra* text accompanying notes 94–98.

43. *See* Kris, *supra* note 9, at 11–12.

44. *See id.* at 12; *see also* NAT'L SECURITY AGENCY, THE NATIONAL SECURITY AGENCY: MISSIONS, AUTHORITIES, OVERSIGHT AND PARTNERSHIPS 5 (2013), *available at* https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf (describing the NSA's process for identifying contacts related to "seed identifier"). At least, that was the NSA's official standard. *See* NAT'L SECURITY AGENCY, *supra*, at 5. According to documents released by Edward Snowden, no specific investigation need be underway; rather the query can merely be part of a broad effort against international terrorism. *See* Glenn Greenwald & James Ball, *The Top Secret Rules that Allow NSA to Use US Data Without a Warrant*, GUARDIAN, June 20, 2013, http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant.

45. *See* President Barack Obama, Speech at the United States Department of Justice (Jan. 17, 2014), *available at* http://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html?_r=0 (stating that "[e]ffective immediately" NSA officials would pursue calls only two steps removed from the seed identifier and indicating that the NSA would have to confirm the seed identifier with the FISC). Legislation proposed by the Obama Administration in March 2014, would incorporate both requirements. *See* Charlie Savage, *Obama to Call for End to N.S.A's Bulk*

part of the process, Judge Leon concluded that the NSA can only figure out the connections between overseas terrorists and people within the United States by canvassing all of the domestic phone and email logs it has collected to see which ones link to the overseas number or email address.[46] But this reasoning only permits a conclusion in favor of standing if the NSA does not have large-scale metadata for the seed identifier's country.[47] In fact, the NSA probably does have such metadata, not only of most people in the U.S. but also of most individuals in many foreign countries.[48] If so, the NSA can simply look at the seed identifier's records rather than sift through every number in its database to see whom the seed has contacted.[49]

A second possible problem with Judge Leon's analysis of the query process could also afflict his analysis of standing to challenge the bulk collection stage. Both procedures are carried out by computers using algorithms.[50] In such cases, humans only see a person's number if a link is established between it and a seed identifier.[51] While Judge Leon quickly dismissed this concern,[52] another court might consider the automated nature

---

Data Collection, N.Y. TIMES, Mar. 24, 2014, http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html (stating that, under the proposed legislation, the FISC would determine "whether the standard of suspicion was met for a particular phone number before the N.S.A. could obtain associated records" and that only two hops would be permitted). *But see infra* note 162.

46. *See Klayman*, 957 F. Supp. 2d at 28.

47. *See id.*

48. *See* Ellen Nakashima & Barton Gellman, *Court Gave NSA Broad Leeway in Surveillance Documents Show*, WASH. POST, June 30, 2014, http://www.washingtonpost.com/world/national-security/court-gave-nsa-broad-leeway-in-surveillance-documents-show/2014/06/30/32b872ec-fae4-11e3-8176-f2c941cf35f1_story.html?Wpisrc =nl%5Feve (stating that the NSA "has been authorized to intercept information 'concerning' all but four countries, according to top-secret documents"); *see also* Barton Gellman & Ashkan Soltani, *NSA Surveillance Program Reaches 'Into the Past' to Retrieve, Replay Phone Calls*, WASH. POST, Mar. 18, 2014, http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html (describing the NSA's MYSTIC surveillance system, which is "capable of recording '100 percent' of a foreign country's telephone calls, enabling the agency to rewind and review conversations as long as a month after they take place").

49. *See Klayman*, 957 F. Supp. 2d at 17–18.

50. *See id.* at 29 n.40 ("The Government contends that 'the mere collection of Plaintiffs' telephony metadata . . . without review of the data pursuant to a query' cannot be considered a search . . . .").

51. *See* NAT'L SECURITY AGENCY, *supra* note 44, at 5 ("Technical controls preclude NSA analysts from seeing any metadata unless it is the result of a query using an approved identifier.").

52. *Klayman*, 957 F. Supp. 2d at 29 n.39 ("It is irrelevant for Fourth Amendment purposes that

of this process highly relevant to whether a litigant can show that he has suffered or will suffer "concrete" injury.[53]

Many of the NSA's other surveillance regimes either do not engage in any bulk collection or appear to follow a more limited version of the two-step collection and query procedure used in the metadata program.[54] If so, proof that a particular plaintiff has suffered or will suffer actual injury will be harder to establish even for challengers of the first-stage data collection process. And, in contrast to Judge Leon's characterization of the metadata query process in *Klayman*, the query process in these other surveillance programs is much more likely to start with the particular "identifier" or "suspect" than with a perusal of the general database,[55] meaning that any given plaintiff will probably be unable to prove that he has been subject to the second stage of the surveillance. In fact, under *Clapper*, when surveillance is covert there is almost an inverse relationship between the intrusiveness of the surveillance visited on a target and the ability of potential targets to obtain standing. If the government covertly zeroes in on the content of person's phone call, email, or bank records, it is usually relying on some type of suspicion, however attenuated, a fact which, by definition, means the query will not have the panvasive nature that bolsters the case for standing vis-a-vis the NSA's bulk collection program. That means that, in the absence of notice, no individual will be able to provide more than "speculation" as to whether he or she has been targeted.

Other possible mechanisms for challenging the metadata program and related programs are unlikely to pick up the slack. Of course, as it has with communications interceptions, Congress could grant standing (and require the predicate notice) to those criminal defendants who are aggrieved by metadata surveillance.[56] But because these programs are even more covert

---

the NSA might sometimes use automated analytical software.").

53. For instance, Judge Posner may disagree with Judge Leon on this point. *See* RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 96–97 (2006) (arguing that when a computer, rather than a human, "sifts" through data, no privacy has been invaded and no potential harm incurred).

54. *See, e.g.*, Goodman *supra* note 13 (describing the "Optic Nerve" program); Goodman, *supra* note 14 (describing the "Turbine" program).

55. *See* Toomey & Kaufman, *supra* note 30, at 885–88 (describing perusal of financial records under Section 215 and perusal of internet activities by the NSA).

56. Congress could even create a right to notice *regardless* of whether prosecution occurs. *Cf.* 18 U.S.C. § 2518(8)(d) (Supp. I 2013) (requiring notice "[w]ithin a reasonable time but not later than ninety days after the filing of an application for an order of approval" except upon "an ex parte

than the Section 702 warrant-based interceptions involved in *Clapper*—and given the government's penchant for engaging in "parallel construction"[57]—the chances of such notice would probably be slim to none.[58] Congress could also create a special advocate in the Foreign Intelligence Surveillance Court to represent the interests of those whose information is queried, a procedure endorsed by President Obama's special commission and included in the administration's recently proposed legislation.[59] But whether such an advocate's office could be counted on to overcome its governmental provenance and the nonchalance that can come from proceeding in secret to develop into a vigorous advocate for individual constitutional claims is at best unclear.[60] Moreover, the advocate's ability to appeal an adverse decision by the FISC is tenuous.[61]

In sum, the federal government is engaged in widespread surveillance that, under current law as construed by the Supreme Court, may not be challengeable as a practical matter. Programs that could be blatantly unconstitutional might be allowed to continue unless and until the legislature

showing of good cause," in which case notice "may be postponed"). However, the Supreme Court is unlikely to constitutionalize such a right to notice. *See* Cady v. Dombrowski, 413 U.S. 433, 449 (1973) (indicating that it is "not . . . constitutionally significant" that a post-search return did not list all discovered items).

57. *See supra* note 29 and accompanying text.

58. Furthermore, trying to use the discovery process to determine whether a prosecution or civil action is based in whole or part on the results of covert surveillance is often stymied by the state secrets defense. *See* Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 GEO. WASH. L. REV. 1249, 1297–99 (2007) (cataloguing cases in which the state secrets defense was raised during the discovery process and concluding that it succeeded far more often than it failed).

59. *See* RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 21 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf ("[W]e recommend that Congress should create the position of Public Interest Advocate to represent the interests of privacy and civil liberties before the FISC.").

60. The history of similar internal oversight mechanisms does not inspire optimism in this regard. *See* SIMON CHESTERMAN, ONE NATION UNDER SURVEILLANCE: A NEW SOCIAL CONTRACT TO DEFEND FREEDOM WITHOUT SACRIFICING LIBERTY 80 (2011) ("Secrecy . . . . may facilitate cover-ups, block investigators, or transform overseers into defenders. . . . [T]here are good reasons to be wary of any structure that relies entirely on government actors.").

61. *See* Stephen I. Vladeck, *Standing and Secret Surveillance*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 551, 575–77 (2014) (noting precedent supporting the conclusion that there is no standing for a "special advocate" appealing a FISC decision).

or the executive branch decides to shut them down.[62] The Supreme Court has made clear that standing need not be granted simply because unconstitutional government action may otherwise be immune from judicial review.[63] But any government practice that has occasioned as much controversy as the NSA's surveillance ought to be subject to such review if a plausible standing argument can be made. The next two parts of this Article proffer such arguments.

III. STANDING IN FOURTH AND FIRST AMENDMENT CASES

Standing doctrine in federal court places a heavy burden on plaintiffs to show that the government action claimed to be illegal had, is having, or will have a direct effect on them. The plaintiff must show a "concrete and particularized" harm that is "actual or imminent, not conjectural or hypothetical," that is "fairly traceable" to the defendant's conduct, and that is "likely" to be redressed by a favorable decision.[64] Additionally, the plaintiff's claim must assert his or her own interest, not the interest of a third party,[65] state something more than a "generalized grievance" aimed merely at assuring the government abides by the law,[66] and fall within the "zone of interests" protected by the relevant statute.[67]

---

62. "Blatantly unconstitutional" is not hyperbole. Perhaps of most note on this score is the fact that Justice Scalia, normally a supporter of law enforcement, called it a "really good question" whether computer data is an "effect" under the Constitution. *See* Debra Cassens Weiss, *Does Fourth Amendment Protect Computer Data? Scalia Says It's a Really Good Question*, A.B.A J. (Mar. 24, 2014, 1:06 PM), www.abajournal.com/news/article/asked_about_nsa_stuff_scalia_says_conversations_arent_protected_by_fourth_a/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email.

63. *See* Schlesinger v. Reservists Comm. to Stop the War, 418 U.S. 208, 227 (1974) ("The assumption that if respondents have no standing to sue, no one would have standing, is not a reason to find standing.").

64. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61, 590 (1992) (internal quotation marks omitted).

65. *See* Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 474 (1982).

66. *See* Warth v. Seldin, 422 U.S. 490, 499 (1975) ("[T]he Court has held that when the asserted harm is a 'generalized grievance' shared in substantially equal measure by all or a large class of citizens, that harm alone normally does not warrant exercise of jurisdiction.").

67. *See* Lujan v. Nat'l Wildlife Fed'n, 497 U.S. 871, 883 (1990). Until recently, the latter three requirements were often said to be "prudential" rather than constitutional in nature, but in the recent decision of *Lexmark International, Inc. v. Static Control Components, Inc.*, 134 S. Ct. 1377 (2014), the Court appeared to abolish that distinction. *See id.* at 1387 n.3.

According to the Supreme Court, these standing requirements exist for two reasons. First, they implement Article III of the Constitution, which limits federal court jurisdiction to certain "Cases" and "Controversies."[68] The case-and-controversy requirement helps ensure that litigants advocate the case diligently, maximizes efficient use of scarce judicial resources, limits judicial inquiries into those matters most conducive to investigation through the adversarial process, and minimizes the issuance of advisory opinions unelucidated by a specific fact pattern.[69] The second reason for the standing requirement, and the one emphasized in *Clapper*, is the desire to prevent "the judicial process from being used to usurp the powers of the political branches."[70] As the Court stated in *Raines v. Byrd*,[71] the Court's standing inquiry "has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional."[72]

In the covert surveillance context, the first rationale should not carry much weight. As in *Clapper*, the parties will often be composed of lawyers and human rights activists, who can be counted on to pursue their constitutional claims aggressively.[73] Amicus briefs can and will fill any gaps in constitutional argumentation left by the parties, at least at the ultimate appellate stages of the litigation.[74] Further, if the challenge is a facial one or

68. *See* U.S. CONST. art. III.

69. *See generally* ERWIN CHEMERINSKY, FEDERAL JURISDICTION 84 (6th ed. 2012).

70. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1146 (2013).

71. 521 U.S. 811 (1997).

72. *Id.* at 819–20; *see also* Antonin Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 SUFFOLK U. L. REV. 881, 881 (1983) ("[S]tanding is a crucial and inseparable element of [the principle of separation of powers], whose disregard will inevitably produce . . . an overjudicialization of the process of self-governance.").

73. The plaintiffs in *Clapper* were "attorneys and human rights, labor, legal, and media organizations whose work allegedly requires them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad" whom the Government had associated with terrorism or with opposition to governments supported by the U.S. *Clapper*, 133 S. Ct. at 1145. *See generally* Mark V. Tushnet, *The "Case or Controversy" Controversy: The Sociology of Article III: A Response to Professor Brilmayer*, 93 HARV. L. REV. 1698 (1980) (arguing that standing doctrine should not bar and should perhaps even facilitate "ideological" litigants).

74. Amicus briefs are filed in well over 70% of all cases heard by the Supreme Court. *See* Paul M. Collins, Jr. & Lisa A. Solowiej, *Interest Group Participation, Competition, and Conflict in the U.S. Supreme Court*, 32 LAW & SOC. INQUIRY 955, 960–61 (2007); *see also* Bruce J. Ennis, *Effective Amicus Briefs*, 33 CATH. U. L. REV. 603, 603 (1984) (noting that "[o]ccasionally, a case will be decided on a ground suggested only by an amicus, not by the parties").

is aimed at the surveillance program as a whole (e.g., an attack on the bulk collection process or on the hop rule[75]), any ambiguity about how the program worked in a particular instance against a particular plaintiff will not affect the ability of the court to resolve the issues raised. If and when the courts determine that the program is constitutional on its face, as-applied challenges could be subject to more demanding standing requirements, analogous to what *Clapper* imposed, or to limitations in the discovery process.[76]

The separation of powers rationale for a narrow standing requirement is the more potent of the two. If judicial review of decisions by the other branches is to be minimized, then a narrow standing doctrine is an effective method of doing so. That is the gravamen of *Clapper*.[77]

Indeed, one could argue that the separation of powers rationale for a narrow standing doctrine is stronger in the context of panvasive surveillance than in many other settings. When a government action affects virtually everyone, the popularly-elected legislative branch could be said to be the best source of any remedy sought.[78] The generalized grievance rule noted above is a means of implementing this notion.[79] It results in a denial of standing when the relief sought "no more directly and tangibly benefits [the plaintiff] than it does the public at large."[80] Thus, the Court has often denied standing in so-called taxpayer lawsuits, as well as in suits involving claims that the environment or other general interests have been harmed by

75. *See supra* text accompanying notes 40–53 (discussing the bulk collection process and the hop rule).

76. *Cf. Clapper*, 133 S. Ct. at 1149 n.4 (noting that, pursuant to hypothetical *in camera* proceedings permitted under 50 U.S.C. § 1806(f) (2012), "the court's postdisclosure decision about whether to dismiss the suit for lack of standing would surely signal to the terrorist whether his name was on the list of surveillance targets."). The state secrets doctrine will often forestall litigation in individual cases. *See* United States v. Reynolds, 345 U.S. 1, 11 (1953) ("Where there is a strong showing of necessity, the claim of privilege should not be lightly accepted, but even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that military secrets are at stake."); *see also supra* note 58 (discussing use of state secrets doctrine to preclude discovery in criminal and civil cases).

77. *See Clapper*, 133 S. Ct. at 1146–47.

78. I have made precisely this argument, albeit with the important caveat that the courts be authorized to monitor the process by which the remedy is constructed. *See infra* note 140 and accompanying text.

79. *See supra* note 66 and accompanying text.

80. Hollingsworth v. Perry, 133 S. Ct. 2652, 2662 (2013).

governmental action or inaction.[81] As the Supreme Court stated in *FEC v. Akins*,[82] "the Court has sometimes determined that where large numbers of Americans suffer alike, the political process, rather than the judicial process, may provide the more appropriate remedy for a widely shared grievance."[83]

When the widely shared grievance has to do with the *proper functioning* of the political process itself, however, the calculus should change. *Akins* itself recognized this point. That case involved a claim that the government had erroneously categorized an organization as a "political committee" for election campaign purposes, resulting in the plaintiffs' inability to force the organization to abide by statutory spending reporting requirements.[84] In deciding that the plaintiffs had standing to pursue this claim, the Court stated that where the asserted injury is "directly related to voting, the most basic of political rights," then "the fact that it is widely shared does not deprive Congress of constitutional power to authorize its vindication in the federal courts."[85] *Akins* suggests that when the plaintiffs' claim is directed at the functioning of the political process rather than at a statute or action that results from that process, standing requirements should be relaxed.

The following discussion explores this idea further in connection with covert surveillance cases. The usual claim on the merits in these cases is based either on the Fourth Amendment, which prohibits unreasonable searches and seizures,[86] or on the First Amendment, which guarantees freedom of speech.[87] *Clapper* holds that plaintiffs who assert that their activities are "chilled" by covert surveillance, but who cannot show that it has caused them actual or impending injury, do not have standing to raise either type of claim.[88] After describing *Clapper's* reasoning and the reasoning of its detractors, this section explains the contribution of political process theory to standing analysis. As developed by John Hart Ely, this theory, applied to standing doctrine, expands on *Akins'* insight and captures better than other rationales why chilling arguments for standing should

81. *See generally* CHEMERINSKY, *supra* note 69, at 91–99 (describing the Court's general hostility to taxpayer lawsuits, as well as citizen suits in environmental matters).

82. 524 U.S. 11 (1998).

83. *Id.* at 23.

84. *See id.* at 11.

85. *Id.* at 12, 25.

86. *See* U.S. CONST. amend. IV.

87. *See* U.S. CONST. amend I.

88. *See infra* text accompanying notes 93–100.

prevail in covert surveillance cases, even when Congress has not, as it did in the statute at issue in *Akins*,[89] authorized suit against the government.

A. Clapper *and Its Detractors*

The *Clapper* plaintiffs wanted to argue that interception of phone calls under section 702 of FISA violated both the Fourth Amendment and the First Amendment.[90] They contended they had standing to make these claims because their concern about having their overseas conversations intercepted by the NSA compromised their ability to "locate witnesses, cultivate sources, obtain information, and communicate confidential information to their clients."[91] They also alleged that, as a result of their concern about the NSA's surveillance, they had "ceased engaging" in phone and email communications with certain people, and that they had undertaken "costly and burdensome measures" to protect confidentiality of their communications.[92] In short, the plaintiffs argued that Section 702 of FISA "chilled" their communications overseas.

The Second Circuit granted standing on the ground that the plaintiffs' fear of surveillance was not "fanciful, paranoid, or otherwise unreasonable."[93] But the Supreme Court disagreed. A five-member majority concluded that "such a fear is insufficient to create standing,"[94] most prominently citing *Laird v. Tatum*,[95] a Supreme Court decision that had denied standing to plaintiffs wanting to challenge what they hypothesized were the military's efforts to investigate and compile dossiers on them.[96] The *Laird* Court concluded that the ability to challenge a government

89. *See* 2 U.S.C. § 437g(a)(1) (2012) ("Any person" who believes FECA [Federal Election Campaign Act] has been violated may file a complaint with the FEC).

90. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1146 (2013). The plaintiffs also argued that section 702 violated Article III's case and controversy requirement and separation of powers principles by allowing the Foreign Intelligence Surveillance Court to issue a warrant in the absence of a case or controversy. *See* Amnesty Int'l USA v. McConnell, 646 F. Supp. 2d 633, 642–43 (S.D.N.Y. 2009), *vacated sub nom.* Amnesty Int'l USA v. Clapper, 638 F.3d 118 (2d Cir. 2011), *rev'd*, 133 S. Ct. 1138 (2013).

91. *Clapper*, 133 S. Ct. at 1145.

92. *Id.* at 1145–46.

93. Amnesty Int'l USA v. Clapper, 638 F.3d 118, 134 (2d Cir. 2011).

94. *Clapper*, 133 S. Ct. at 1152.

95. 408 U.S. 1 (1972).

96. *Id.* at 2.

surveillance practice cannot be derived from a "chilling effect aris[ing] merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some *other* and additional action detrimental to that individual."[97] Taken literally, this language would deny standing not only on *Clapper's* facts, but even if the plaintiffs *had* been able to show that their calls had been intercepted;[98] only use of the intercepts against them would trigger standing under *Laird*.

Whether the Court meant to sanction that result is not clear. But at a minimum *Clapper* and *Laird* appear to firmly reject any standing argument based on the claim that the challenged government program inhibits certain types of behavior, absent a further showing that the government has or "certainly" will take more direct action against the challengers.[99] That the Court really meant "certainly" was brought home by the fact that it refused to find standing despite the dissent's persuasive arguments that there was a "very high likelihood" the government had used and would continue to use section 702 as authority to intercept at least some of the plaintiffs' communications.[100]

What the majority failed to recognize is that, while the chilling effect described by the *Clapper* plaintiffs did not definitively prove their calls had been intercepted, it "certainly" undermined the political process that, according to *Clapper*, standing doctrine is meant to protect.[101] Two recent articles provide the building blocks for this argument.

Consider, first, Professor Luke Milligan's interpretation of the first eight words of the Fourth Amendment, to wit, "[t]he right of the people to be secure" against unreasonable searches and seizures.[102] Pointing to colonial dictionaries, case law, legislation and literature, Professor Milligan argues that the Fourth Amendment's choice of the words "[t]he right of the people" and "to be secure," combined with the colonists' clear disdain for general warrants, demonstrates that the framers were as worried about the

97. *Id.* at 11.

98. *See id.* at 11 (stating that "the complainant [must be] either presently or prospectively subject to the regulations, proscriptions, or compulsions that he [is] challenging").

99. *See Clapper*, 133 S. Ct. at 1152; *Laird*, 408 U.S. at 11–13.

100. *See Clapper*, 133 S. Ct. at 1157–60 (Breyer, J., dissenting).

101. *See id.* at 1146 (majority opinion).

102. Luke M. Milligan, *The Forgotten Right to Be Secure*, 65 HASTINGS L.J. 713 (2014).

oppression caused by a *regime* of unreasonable searches as they were about preventing particular searches.[103] Thus, contrary to the Court's statements in *Clapper* and *Laird*, Professor Milligan concludes that the Constitution guarantees not only freedom from unreasonable searches and seizures but also freedom from the *fear* of such searches and seizures.[104] In other words, the Fourth Amendment's history, structure and text demonstrate that the Fourth Amendment has preemptive as well as sanctioning power.

Acceptance of that argument does not necessarily mean that every United States citizen ought to have standing to challenge a statute on a chilling theory. To assure the efficient use of judicial resources, adequate advocacy and the other positive attributes associated with the case and controversy requirement, plaintiffs should have to show, as the plaintiffs in *Clapper* did,[105] that the government has officially adopted an unregulated surveillance program that has affected their communications in specifiable ways. More specifically, plaintiffs should only have standing if they can show: (1) the existence of a surveillance program that does not adhere to traditional Fourth Amendment constraints (i.e., a warrant based on particularized probable cause),[106] which (2) causes a significant, concrete and reasonable (i.e., not a "fanciful" or "paranoid") modification of the plaintiffs' typical methods of communicating with other people, particularly (given the Fourth Amendment's focus) their private methods of communicating. For prudential reasons, the plaintiffs might also be required to demonstrate that (3) the inhibited activity is not criminal in nature and that (4) the covert nature of the surveillance program means that it is not likely to be challenged through another judicial forum.

A similar rule might be derived from the First Amendment's language stating that freedom of speech and association should not be "abridg[ed]."[107] To abridge means "to lessen the strength or effect of."[108] As many scholars

103. *Id.* at 737–49 (canvassing colonial definitions and uses of the word "secure," analyzing the "structure of the fourth amendment," and discussing colonial "discourse" about the general warrant prohibition).

104. *Id.* at 749–50 ("[F]ounding-era discourse strongly suggests that, in the context of unreasonable searches and seizures, the framers realized the value of 'protection' and 'freedom from fear.'").

105. *See* 133 S. Ct. at 1145–46.

106. *See* sources cited *supra* note 2.

107. U.S. CONST. amend. I.

108. *Abridge Definition*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/abridge (last visited Nov. 29, 2014).

have noted, surveillance has precisely that effect on communication and related activities.[109] Professor Neil Richards has recently argued, for instance, that "the fear of being watched causes people to act and think differently from the way they might otherwise."[110] A considerable empirical literature backs up the claim that "panvasive surveillance" leads individuals "to make choices that conform to mainstream expectations."[111] Because unconstrained surveillance can lead to "self-censorship, in terms of speech, action, or even belief," Richards contends that people should have standing to challenge this type of surveillance on First Amendment grounds.[112] Although Richards does not go into any detail about the specifics of this standing proposal, the above Fourth Amendment formulation might work

109. *See, e.g.*, Dawinder S. Sidhu, *The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans*, 7 U. MD. L.J. RACE, RELIGION, GENDER & CLASS 375, 375–76 (2007) (describing the chilling effect of surveillance on members of minority ethnic, religious, and political communities); Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 745–46 (2008) (arguing that the uncertainty about whether one is subject to surveillance inhibits direct associations with controversial groups and those affiliated with such groups or who seem otherwise likely to come under suspicion).

110. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1948 (2013). I have made a similar argument in SLOBOGIN, *supra* note 20, at 98–101. See also Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 252–58 (2002), for a discussion of lower court and NLRB cases that find chilling arguments cognizable, and of Supreme Court case law protecting the right to anonymity as a means of protecting expressive conduct.

111. Richards, *supra* note 110, at 1949 (internal quotation mark omitted); *see also* Alex Marthews & Katherine Tucker, Government Surveillance and Internet Search Behavior (Aug. 28, 2014) (unpublished manuscript), *available at* http://ssrn.com/abstract=2412564 (finding, in the wake of Edward Snowden's revelations, a statistically significant reduction in use of search terms that might appear suspicious to the U.S. government); GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE 178–86 (2014) (describing social science research from the U.S., U.K., and Finland, and the experience of journalists and Muslims post-9/11, suggesting that "the effect of being watched is to severely constrain individual choice"); Carl Botan, *Communication Work and Electronic Surveillance: A Model for Predicting Panoptic Effects*, 63 COMM. MONOGRAPHS 308–09 (1996) ("[E]mployees who are surveilled . . . experience . . . a reduced sense of privacy, increased uncertainty [as to job security], and reduced communication."); Carl Botan & Michaela Vorvoreanu, "What Are You Really Saying to Me?": Electronic Surveillance in the Workplace 9–10 (June 2000) (unpublished manuscript), *available at* http://www.antoniocasella.eu/nume/Botan_2000.pdf ("[T]he overwhelming meta-message that surveillance seems to send to employees is that they are distrusted . . . and heavily surveilled employees reported reduced motivation to do more *quantity* of work . . . and reduced motivation to do higher *quality* work [as well as] reduced loyalty to the organization, increased stress at work, and reduced enthusiasm about even going to work . . . ."); *infra* notes 121–30 and accompanying text.

112. Richards, *supra* note 110, at 1949.

just as well in the First Amendment context.

The arguments from Professors Milligan and Richards are the beginning of a rejoinder to the Court's decision in *Clapper*. But one might still ask how their arguments are, at bottom, any different from the chilling argument rejected by the Court in *Clapper* and *Laird*. Without further elaboration, they are not. What is needed is an explanation of why unregulated surveillance undermines the political system that standing doctrine ostensibly is meant to preserve.

B. Standing Under Political Process Theory

The political process theory of constitutional interpretation might provide such an explanation. As laid out by John Hart Ely in *Democracy and Distrust*, political process theory dictates a narrow vision of judicial review when courts are interpreting vague provisions like the Equal Protection and Due Process Clauses.[113] But while Ely thought courts should resist gleaning substantive meaning from amorphous constitutional language, he argued that courts should still be quite willing to protect "participational values" associated with voting, political involvement, government transparency, and the like.[114] Those are the values, Ely argued, "(1) with which our Constitution has preeminently and most successfully concerned itself, (2) whose 'imposition' is not incompatible with, but on the contrary supports, the American system of representative democracy, and (3) that courts set apart from the political process are uniquely situated to 'impose.'"[115] According to Ely, the Constitution establishes "a process of government," to wit, representative democracy.[116]

The role of the judiciary in this constitutional scheme is to discern when the democratic process is not functioning properly. Echoing the language in footnote four of *United States v. Carolene Products Co.*,[117] Ely emphasized that any legislative or executive action that undermines interests "essential to political participation" should be declared unconstitutional by the courts.[118] As developed in the next section, this language describes a separation of

113. *See* JOHN HART ELY, DEMOCRACY AND DISTRUST (1980).
114. *Id.* at 75 n.*.
115. *Id.*
116. *Id.* at 101.
117. 304 U.S. 144, 152 n.4 (1938).
118. ELY, *supra* note 113, at 136.

powers principle that could provide a *merits* ground, independent of the Fourth and First Amendments, for challenging certain types of government actions. But it also is relevant to standing analysis; more specifically, it anticipates the holding in *Akins*,[119] without the constricting requirement that Congress authorize the suit. Political process theory dictates that citizens whose participation in the political process is concretely affected by a government action should be able to challenge it.

If one adopts this political process perspective in thinking about standing to challenge covert practices like the NSA's metadata program, the question then becomes how covert surveillance might affect this participation. Professor Richards provides a hint with his observation that "unconstrained surveillance, especially of our intellectual activities, threatens a cognitive revolution that cuts at the core of the freedom of the mind that our political institutions presuppose."[120] This is a chilling argument, but a chilling argument framed in terms of its impact on the political process, not on individual rights.

That different framing should make a difference in standing analysis. As the plaintiffs' reactions in *Clapper* demonstrate, political participation can be compromised by legitimate fears concerning covert surveillance.[121] Even more significantly, the Fourth Estate, crucial to maintaining a vibrant democracy, has been affected by the government's surveillance practices. A 2013 survey of journalists and other writers found that, in the wake of Snowden's disclosures, "24% have deliberately avoided certain topics in phone or email conversations."[122] A more recent report, based on a survey of forty-six journalists and forty-two lawyers, concluded that "journalists and their sources, as well as lawyers and their clients, are changing their

119. FEC v. Akins, 524 U.S. 11 (1998) (granting taxpayers the standing to sue the FEC for misclassifying a political organization).

120. Richards, *supra* note 110, at 1964.

121. *See, e.g.*, Beatrice Edwards, *The Government-Corporate Complex: Surveillance for the Money*, TRUTHOUT (May 27, 2014, 1:39 PM), http://www.truth-out.org/news/item/23969 (describing how, in the wake of Snowden's revelations, the author and her colleagues at a small Washington, D.C. nonprofit organization law firm that defends whistle-blowers "have to talk face to face as if we were subversives"). *See generally* JULES BOYCOFF, THE SUPPRESSION OF DISSENT: HOW THE STATE AND MASS MEDIA SQUELCH US AMERICAN SOCIAL MOVEMENTS 109–26 (2006) (describing, inter alia, "pervasive self-censorship" due to fear of surveillance, including speaking softly and avoiding meetings, by those close to Martin Luther King).

122. PEN AM. CTR., CHILLING EFFECTS: NSA SURVEILLANCE DRIVES U.S. WRITERS TO SELF-CENSOR 6 (2013), *available at* http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.

behavior in ways that undermine basic rights and corrode democratic processes."[123] This report noted that "[s]everal journalists likened the current reporting atmosphere to what one might find in more authoritarian countries."[124]

Perhaps most significantly, surveillance can compromise the political process even at the upper reaches of government. In March 2014, for instance, Senator Dianne Feinstein, chair of the Senate Select Intelligence Committee, complained about suspected (but unproven) CIA hacking into her office computers.[125] Under *Clapper*, she would not have standing to bring a claim against the CIA. But in drafting emails and documents the Senator and her staff undoubtedly now think twice about what they are saying, especially about executive branch powers. This chilling effect is the kind of concrete impact that should lead to standing under political process theory. As Senator Feinstein stated in reaction to the incident, "[T]he CIA's search may well have violated the separation of powers principles embodied in the U.S. Constitution, including the speech and debate clause. It may have undermined the constitutional framework essential to effective congressional oversight of intelligence activities or any other government function."[126]

Along the same lines, commentators have speculated that members of Congress have curbed their efforts to regulate surveillance because of their fear of it.[127] Some have even suggested that President Obama has been

123. AM. CIVIL LIBERTIES UNION & HUMAN RIGHTS WATCH, WITH LIBERTY TO MONITOR ALL: HOW LARGE-SCALE US SURVEILLANCE IS HARMING JOURNALISM, LAW, AND AMERICAN DEMOCRACY 1 (2014), *available at* https://www.aclu.org/sites/default/files/assets/dem14-withliberty tomonitorall-07282014.pdf.

124. *Id.* at 47.

125. 160 CONG. REC. S1487-07 (daily ed. Mar. 11, 2014) (statement of Sen. Dianne Feinstein), 2014 WL 940817, *available at* http://www.washingtonpost.com/world/national-security/transcript-sen-dianne-feinstein-says-cia-searched-intelligence-committee-computers/2014/03/11/200dc9ac-a928-11e3-8599-ce7295b6851c_story.html.

126. *Id.* Note Senator Feinstein's reference to the Speech and Debate Clause, which protects against inquiry into the motivation for federal legislative acts. *See* United States v. Brewster, 408 U.S. 501, 525 (1972). That clause further bolsters the political process case for standing when covert surveillance is aimed at legislators.

127. *See, e.g.*, McGovern, *supra* note 29 (suggesting that one explanation for the recent dissipation of congressional outrage at the bulk collection process is "the possibility of blackmail or at least the fear among some politicians that the NSA has collected information on their personal activities that could be transformed into a devastating scandal if leaked at the right moment").

similarly constrained.[128] Glenn Greenwald summarized the impact of secret panvasive surveillance as "the ultimate imbalance, permitting the most dangerous of all human conditions: the exercise of limitless power with no transparency or accountability."[129]

In contrast, the types of suits that are typically stymied by standing requirements do not seek to protect the pillars of democracy. Claims alleging environmental damage or misuse of taxpayer funds raise important issues. But they are not aimed at protecting the integrity of the political process. Challenges to covert surveillance ultimately address the structure of government, not its products.[130]

IV. A THIRD BASIS FOR CHALLENGING SURVEILLANCE: SEPARATION OF POWERS AND THE NONDELEGATION DOCTRINE

One response to standing arguments based on the insights of scholars like Milligan and Richards is that they ignore the close relationship between standing and the scope of the right in question.[131] Indeed, when the Fourth Amendment is the basis for the claim, the Supreme Court has explicitly conflated standing with the Amendment's substance. In *Rakas v. Illinois*,[132]

128. *See, e.g.*, William Greider, *Is the NSA Eavesdropping on President Obama?*, NATION (Oct. 29, 2013, 1:12 PM), http://www.thenation.com/blog/176879/nsa-eavesdropping-president-obama ("If Obama fiddles around with inquiries that do not change much of any[th]ing for the spy masters, then the president himself may be incorporated in the suspicions. Some people will ask: what did the NSA or CIA have on Obama?").

129. GREENWALD, *supra* note 111, at 169. The practical impact of inter-branch distrust was also captured by ex-President Jimmy Carter's recent admission that he communicates with foreign leaders via snail mail on the assumption that his electronic communications are monitored by the NSA. *See* Dana Davidsen, *Jimmy Carter Believes the NSA Monitors His E-Mails*, CNN.COM (Mar. 23, 2014, 1:47 PM), http://politicalticker.blogs.cnn.com/2014/03/23/jimmy-carter-believes-the-nsa-monitors-his-e-mails/.

130. *See* Michael J. Glennon, *National Security and Double Government*, 5 HARV. NAT'L SECURITY J. 1, 89 (2014) ("[T]he organizations in question 'do not regulate truck widths or set train schedules. They have the capability of radically and permanently altering the political and legal contours of our society.' An unrestrained security apparatus has throughout history been one of the principal reasons that free governments have failed." (footnote omitted) (quoting Michael J. Glennon, *Investigating Intelligence Activities: The Process of Getting Information for Congress*, *in* THE TETHERED PRESIDENCY: CONGRESSIONAL RESTRAINTS ON EXECUTIVE POWER 152 (Thomas M. Franck ed., 1981))).

131. *Cf.* William A. Fletcher, *The Structure of Standing*, 98 YALE L.J. 221, 224 (1988) ("If a duty is constitutional, the constitutional clause should be seen not only as the source of the duty, but also as the primary description of those entitled to enforce it.").

132. 439 U.S. 128 (1978).

the Court stated that the decision as to whether a defendant can make a Fourth Amendment claim "forthrightly focuses on the extent of a particular defendant's rights under the Fourth Amendment, rather than on any theoretically separate, but invariably intertwined concept of standing."[133] If a government action is not a Fourth Amendment "search" vis-à-vis the litigant, *Rakas* held, then the litigant lacks standing to challenge it.

If that reasoning is the correct approach to standing, then in cases challenging covert surveillance on Fourth or First Amendment grounds everything rides on whether the surveillance, as it operates in the way the plaintiff describes it, infringes the plaintiff's reasonable expectations of privacy or speech and association interests.[134] While such a finding would presumably be made in the *Clapper* case, which involved the alleged interception of the content of overseas phone calls,[135] it is less certain in connection with collection and querying of metadata. The Fourth Amendment is only meant to protect *reasonable* expectations of privacy.[136] Supreme Court case law to date strongly suggests that any privacy one might expect in one's metadata or Internet activity is unreasonable, because we assume the risk that third parties to which we knowingly impart information (here phone companies and Internet service providers) will in turn divulge it to the government.[137]

The same type of analysis might limit standing in cases brought under the First Amendment. As the Court intimated in *Clapper*,[138] one could conclude that even if speech and association are inhibited by surveillance, that inhibition proximately results from the *individual's* choices, not from

133. *Id.* at 139.

134. For Fourth and First Amendment arguments, see SLOBOGIN, *supra* note 20, at 98–101, 180–96.

135. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143–44 (2013).

136. *See, e.g.*, Jones v. United States, 132 S. Ct. 945, 950 (2012) ("Our . . . cases have . . . said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.'").

137. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979) ("[P]etitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. . . . [He thereby] assumed the risk that the company would reveal to police the numbers he dialed."); United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

138. 133 S. Ct. at 1151 ("[R]espondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.").

anything the government has done to the individual.[139] On this view, even if an individual can show that he or she was targeted, standing to contest surveillance does not exist unless and until the government uses the seized information against the individual, because otherwise a colorable claim that a constitutionally cognizable interest was infringed cannot be made.

If, despite its impact on political participation, covert surveillance like the metadata program remains immune from Fourth and First Amendment challenges, there remains another avenue of attack, derived directly from separation of powers doctrine. In other work, I have argued that, even if the Fourth (or First) Amendment does not govern a particular type of surveillance, Ely's political process theory provides a basis for challenging panvasive actions that are the result of a seriously flawed political process.[140] More specifically, panvasive surveillance might be challengeable on one of three grounds: (1) the surveillance is not authorized by the appropriate legislative body; (2) the authorizing legislative body does not meaningfully represent the group affected by the surveillance; or (3) the resulting legislation or law enforcement's implementation of it violates notions underlying the non-delegation doctrine.[141] The first and third of these grounds are based explicitly on separation of powers concerns.

As I pointed out, some panvasive surveillance has not been legislatively authorized or has been authorized by legislation that does not announce an "intelligible principle" governing the implementing agency.[142] Panvasive surveillance is also defective under non-delegation principles if, as I have argued is true of the NSA's metadata program, it is implemented by rules or practices that are not explained, were produced through flawed or non-transparent procedures, or are applied unevenly.[143] Based on several Supreme Court cases, particularly in the administrative law area,[144] I

139. *See, e.g.*, ACLU v. NSA, 493 F.3d 644, 656–57 (6th Cir. 2007) ("[B]y proposing only injuries that *result* from this refusal to engage in communications (e.g., the inability to conduct their professions without added burden and expense), [plaintiffs] attempt to supplant an insufficient, speculative injury with an injury that appears sufficiently imminent and concrete, but is only incidental to the alleged wrong (i.e., the NSA's conduct) . . . ." (footnote omitted)).

140. *See* Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721 (2014).

141. *Id.* at 1737.

142. *Id.* at 1766–67 (discussing the lack of legislative authorization for fusion centers).

143. *Id.* at 1753–54, 1755–58 (discussing flawed implementation of rules governing camera surveillance and of the NSA program).

144. *Id.* at 1760–61 (discussing, *inter alia*, SEC v. Chenery Corp., 332 U.S. 194 (1947), Motor

concluded that any one of these deficiencies could be the basis for the claim that the legislature, the relevant law enforcement agency, or both are failing to carry out their constitutional obligations as law-making and law-implementing bodies.[145]

Although this type of claim, like the Fourth and First Amendment claims, aims at "generalized relief," the Court itself has often granted standing to individuals making separation of powers claims.[146] The rationale of these cases is not difficult to grasp, because it again reflects the political process rationale. Many years ago Justice Brandeis stated, "[T]he doctrine of the separation of powers was adopted by the convention of 1787 not to promote efficiency but to preclude the exercise of arbitrary power."[147] More recently, Chief Justice Burger asserted that "checks and balances were the foundation of a structure of government that would protect liberty."[148] More recently still, in *Bond v. United States*[149] the Court stated "[t]he structural principles secured by the separation of powers protect the individual as well."[150]

If one accepts the possibility that a separation of powers argument can be made in covert surveillance cases, then parties who can demonstrate the type of injury described above—that is, a significant stifling of political participation that, to borrow the Second Circuit's language in its *Clapper* decision,[151] is a reasonable, non-fanciful, and non-paranoid reaction to covert surveillance—should have standing to challenge panvasive surveillance even if it is not a search under the Fourth Amendment or does not abridge First

---

Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29 (1983), and United States *ex rel.* Accardi v. Shaughnessy, 347 U.S. 260 (1954), and arguing that these cases hold that administrative rules must be justified on transparent grounds, be substantively reasonable and well-grounded in facts, and be binding on agencies when developed through the process described in § 553 of the Administrative Procedure Act, 5 U.S.C. § 553 (Supp. I 2013)).

145. *Id.* at 1764–65.

146. *See generally* William Marks, Note, Bond, Buckley, *and the Boundaries of Separation of Powers Standing*, 67 VAND. L. REV. 505, 516 (2014) ("Given its concern with individual rights, the Court in recent years has routinely entertained separation of powers cases . . . . The Court has permitted these suits because the alleged injuries are the precise infringements of liberty that the Framers sought to prevent when ensuring federal power was diffuse.").

147. Myers v. United States, 272 U.S. 52, 293 (1926) (Brandeis, J., dissenting).

148. Bowsher v. Synar, 478 U.S. 714, 722 (1986).

149. 131 S. Ct. 2355 (2011).

150. *Id.* at 2365.

151. *See* Amnesty Int'l USA v. Clapper, 638 F.3d 118, 134 (2d Cir. 2011), *rev'd*, 133 S. Ct. 1138 (2013).

Amendment freedom. The merits claim would not be that the surveillance is an unreasonable search or infringement of speech or association rights, but rather that the legislature has failed in its delegation task or that the relevant law enforcement or intelligence agency has acted in an ultra vires fashion. These are the types of separation of powers claims that courts ought to hear because they assure the proper functioning of the political process that the Court is so eager to protect (with, *inter alia*, its standing doctrine). To requote Chief Justice Roberts, "[T]he obligation of the Judiciary [is] not only to confine itself to its proper role, but to ensure that the other branches do so as well."[152]

V. OBJECTIONS

One objection to the political process rationale for granting standing to litigants with colorable claims of injury from NSA surveillance is that, as *Clapper* stated, the Court has "often found a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs."[153] A separate but related objection comes from Professor Jesse Choper, who argued in 1980 that the executive and legislative branches have "tremendous incentives jealously to guard [their] constitutional boundaries and assigned prerogatives against invasion by the other," and thus separation of powers issues ought to be non-justiciable political questions.[154]

Neither of these objections are sustainable from the political process perspective. Precisely because of the perceived importance of national security, the legislative and executive branches often either act in collusion with one another or, as illustrated earlier, function in ways that undermine the other's prerogatives, with the result that both end up ignoring their constitutional obligations.[155] Particularly when it comes to national security,

152. City of Arlington v. FCC, 133 S. Ct. 1863, 1886 (2013) (Roberts, C.J., dissenting).

153. 133 S. Ct. at 1147.

154. JESSE H. CHOPER, JUDICIAL REVIEW AND THE NATIONAL POLITICAL PROCESS 275 (1980).

155. *See, e.g.*, *supra* text accompanying notes 125–26 (discussing Senator Dianne Feinstein's allegations that the CIA hacked computers used by the Senate Select Intelligence Committee); *see also* Emily Arthur Cardy, Note, *The Unconstitutionality of the Protect America Act of 2007*, 18 B.U. PUB. INT. L.J. 171, 179 (2008) (arguing that in passing the Protect America Act, which, *inter alia*, permitted domestic spying by the NSA, "Congress abdicated its responsibility to act as a check on Executive power"); Anjali Dalal, Administrative Constitutionalism and the Re-Entrenchment of Surveillance Culture 3–24 (Mar. 4, 2013) (unpublished manuscript), *available at*

courts should have the authority to ensure that legislatures define the scope of permissible law enforcement and that law enforcement abide by appropriate rule-making mechanisms, a notion the Court has accepted in related national security contexts.[156] At the least, these obligations should include procedures for assuring public accountability (such as notice-and-comment or other transparent rule-making processes), or, if that is not feasible, some method of assuring accountability to the legislature.[157] Unfortunately, the perceived imperatives of the War on Terrorism have led both branches to short-circuit these requirements.[158]

A different kind of objection is that the political process rationale for standing reaches too broadly.[159] If the chilling effect of panvasive surveillance on private communications and speech and association is enough to establish standing, then other challenges to alleged flaws in the political process—ranging from voting matters to educational obligations—could conceivably create standing as well. Perhaps so. As noted above,[160] in *FEC v. Akins* the Court has already recognized as much with respect to the "most basic of political rights" of voting.[161] Whether other interests less

http://ssrn.com/abstract=2236502 (describing government surveillance from the era of J. Edgar Hoover to the present, and pointing out the ease with which intra-agency, inter-agency, and congressional oversight was co-opted by the perceived exigencies of crime-fighting and detecting threats).

156. *See* Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004) (stating, in finding that enemy combatants are entitled to due process, that "[w]hatever power the United States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, it most assuredly envisions a role for all three branches when individual liberties are at stake").

157. *See* Slobogin, *supra* note 140, at 1775 (arguing that "[l]aw enforcement agencies . . . should be encouraged to engage in rulemaking" and that the rules that emerge "should be accompanied by reasons for their interpretations of authorizing legislation, those interpretations must be reasonable, and the rule-creating process must follow some sort of formal procedure, preferably allowing for comments by the people affected").

158. *See* DANA PRIEST & WILLIAM M. ARKIN, TOP SECRET AMERICA: THE RISE OF THE NEW AMERICAN SECURITY STATE xix (2011) (arguing that, because of secrecy and lack of oversight, the U.S. government "has still not engaged the American people in an honest conversation about terrorism and the appropriate U.S. response to it"); McGovern, *supra* note 29 ("The Separation of Powers designed by the Constitution's Framers to prevent excessive accumulation of power by one of the branches has stopped functioning amid the modern concept of 'permanent war' and the unwillingness of all but a few hearty souls to challenge the invocation of 'national security.'").

159. *Cf.* Fletcher, *supra* note 131, at 250 ("If standing to sue is seen as a question of law on the merits, a determination of who should be entitled to judicial enforcement depends on the particular legal right at issue.").

160. *See supra* text accompanying notes 84–85.

161. 524 U.S. 11, 12 (1998).

closely related to the democratic process might be treated similarly is beyond the scope of this Article.

VI. CONCLUSION

If panvasive surveillance cannot be challenged in court, it could well continue indefinitely despite its real threat to democratic institutions. Despite all of the hullabaloo occasioned by Edward Snowden's disclosures, the NSA appears to be continuing its large-scale surveillance and Congress has yet to propose serious limitations on it.[162] Although President Obama has put a few new restrictions on the NSA's programs,[163] to date there have been few judicial assessments of their constitutional status, and *Clapper* stands as an obstacle to challenges to all but the most obviously panvasive government actions.

While the limitations on standing may make sense in some types of cases, challenges to panvasive surveillance should be treated differently than most other generalized claims. The separation of powers, Fourth Amendment, and First Amendment concerns about this surveillance go to the core of American democracy. The Court's decision in *De Jonge v. Oregon*, decided almost eight decades ago, makes the point in language that still resonates in this post-9/11 era:

> The greater the importance of safeguarding the community from incitements to the overthrow of our institutions by force and violence, the more imperative is the need to preserve inviolate the

162. Congress has yet to pass the administration's bill limiting the metadata program, *see supra* note 45, and the administration has not substantially changed the program despite having the authority to do so on its own. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, RECOMMENDATION ASSESSMENT REPORT 3–15 (2015), *available at* http://www.pclob.gov/library/Recommendations_Assessment-Report.pdf (noting these facts and stating that most of the recommendations from the Board that were designed to increase transparency and limit targeting, while "accepted" by the administration, have either not been implemented, have been implemented only "in part," or are in the process of being implemented). In June 2014, the House passed a bill purporting to limit significantly the metadata program, but a close inspection of the bill indicates otherwise. *See* Lizabeth Paulat, *That Surveillance Reform Bill Was Gutted, Passed and Sent to the Senate*, TRUTHOUT (June 2, 2014, 9:08 AM), http://www.truth-out.org/opinion/item/24070-that-surviellance-reform-bill-was-gutted-passed-and-sent-to-the-senate (stating that House amendments to the USA Freedom Act, meant to regulate the NSA's surveillance practices, "took a bill, which was already being criticized as slightly weak, and made it almost wholly ineffective").

163. *See supra* note 45.

> constitutional rights of free speech, free press and free assembly in order to maintain the opportunity for free political discussion, to the end that government may be responsive to the will of the people and that changes, if desired, may be obtained by peaceful means. Therein lies the security of the Republic, the very foundation of constitutional government.[164]

Unwarranted surveillance broadly stifles fundamental liberties and undermines "the very foundation of constitutional government." Government is no longer functioning as the framers of the Constitution imagined it should if political discourse, individual creativity, outspokenness and non-conformity are not allowed to flourish. This state of affairs threatens rather than sustains the notion of separate but equal governmental powers, because it diminishes the vitality of the legislative function, improperly enhances the executive function, and ignores the judiciary's role as a regulator of law enforcement through determinations of cause. Standing doctrine, meant to ensure each branch of government is allowed to do its job, should not prevent courts from ensuring that the other branches actually do it.

164. 299 U.S. 353, 365 (1937).