DePaul Law Review

Volume 66
Issue 2 *Winter 2017: Twenty-Second Annual Clifford Symposium on Tort Law and Social Policy*

Article 5

Standing After Snowden: Lessons on Privacy Harm from National Security Surveillance Litigation

Margot E. Kaminski

STANDING AFTER SNOWDEN: LESSONS ON PRIVACY HARM FROM NATIONAL SECURITY SURVEILLANCE LITIGATION

*Margot E. Kaminski**

ABSTRACT

Article III standing is difficult to achieve in the context of data security and data privacy claims. Injury in fact must be "concrete," "particularized," and "actual or imminent"—all characteristics that are challenging to meet with information harms. This Article suggests looking to an unusual source for clarification on privacy and standing: recent national security surveillance litigation. There we can find significant discussions of what rises to the level of Article III injury in fact. The answers may be surprising: the interception of sensitive information; the seizure of less sensitive information and housing of it in a database for analysis; and harms arising from data analytics have all been taken seriously in recent national security cases. This Article closes by noting that no discussion of corporate responsibility and data theft can be complete without addressing the roles corporations play in challenging the national security state.

I. INTRODUCTION

Data security is a significant problem. In 2013, forty million customer credit card numbers were taken from the retail giant Target.[1] The Target hack yielded seventy million records with shoppers' names, addresses, email addresses, and phone numbers.[2] In 2015, the extramarital hookup website Ashley Madison was hacked for identifying information about its thirty-seven million users.[3] Also in 2015, the Office of Personnel Management (OPM) data breach revealed the So-

* Assistant Professor of Law at The Ohio State University Moritz College of Law. Thanks to Paul Ohm for workshopping this at an earlier stage, and to my fellow panelists Andrea Matwyshyn and Felix Wu.

1. Brian Krebs, *The Target Breach, by the Numbers*, KREBS ON SECURITY (May 6, 2014), http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.

2. *Id*.

3. *Id*.

cial Security Numbers of an estimated 21.5 million people, and the fingerprint records of an estimated 5.6 million people.[4]

Discussions of corporate and governmental responsibility have no doubt increased in the wake of these events, each of which has come with a high price tag for cleaning up the aftermath. Yet the U.S. legal system stumbles in assigning responsibility for data harms. The first-order hurdle—recently addressed by the Supreme Court in *Spokeo, Inc. v. Robins*[5]—is standing. What harm must a person show to get a data breach case in front of a court?

Standing to sue is one of the larger problems for both data breach and data privacy litigation. As one court explained, "even though injury-in-fact may not generally be Mount Everest . . . in data privacy cases . . . the doctrine might still reasonably be described as Kilimanjaro."[6] Lower courts struggle with standing in data breach and data privacy cases, and have produced varied results.[7] Courts, desperate to find something tangible, sometimes resort to looking to more measurable proxies for injury, such as increased cellular phone battery usage when an app repeatedly requests updates on a user.[8] These proxies do not indicate where real privacy harms lie. How can courts better determine when a plaintiff gets into court?

---

4. Keith Wagstaff et al., *OPM: 21.5 Million People Affected by Background Check Breach*, NBC NEWS (July 9, 2015, 8:12 PM), http://www.nbcnews.com/tech/security/opm-hack-security-breach-n389476; *see also* Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, WASH. POST (Sept. 23, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/. It now appears that the OPM breach included not only background check information, but also security clearance information with details about employees' personal lives, including law enforcement records, polygraph data and information about journalists who had access to federal buildings. *See* Michael Adams, *Why the OPM Hack Is Far Worse than You Imagine*, LAWFARE (Mar. 11, 2016, 10:00 AM), https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine; Lisa Rein, *The Chinese Didn't Just Hack Federal Employees. Journalists Were Swept Up in the Massive Breach, Too*, WASH. POST (Dec. 14, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/12/14/the-chinese-didnt-just-hack-federal-employees-journalists-were-swept-up-in-the-massive-breach-too/.

5. 136 S. Ct. 1540 (2016).

6. In re Google Inc. Privacy Policy Litigation, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013).

7. *Compare* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (finding standing), *and In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1218 (N.D. Cal. 2014), *with* Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (denying standing), Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011), Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 640 (7th Cir. 2007), *In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 108 F. Supp. 3d 949, 962 (D. Nev. 2015), Green v. eBay Inc., 2015 WL 2066531, at *2 (E.D. La. May 4, 2015), *and* Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 649 (S.D. Ohio 2014).

8. *See In re* Google Android Consumer Privacy Litig., 2013 WL 1283236, at *5 (N.D. Cal. Mar. 26, 2013) (finding standing to sue Google for changes to its privacy policy on the basis of increased cell battery usage).

To answer this question, this Article turns to a source often overlooked in these conversations: national security litigation. At first glance, this may seem like a terrible idea. Courts historically have been highly deferential to the government over national security claims. Looking to these standards to clarify standing in the private sector context could produce results that skew heavily against plaintiffs.

However, in the years since 2013, when security contractor Edward Snowden revealed information about U.S. national security surveillance,[9] U.S. courts have repeatedly confronted both standing and privacy harm in the context of national security surveillance litigation. The ensuing discussions of standing, arising around the First and Fourth Amendments, can provide valuable insights for the discussion of standing and data breaches in the private sector context.

This Article's closing claim is more normative. National security litigation can actually be an important component of corporate responsibility. Just as corporations can develop tools to provide security against government surveillance, they can and should sue the government on behalf of themselves and, sometimes, their customers. Corporations are often better situated than most individuals to sue. They have deep pockets; moreover, they are better situated under current doctrine because they can articulate claims on behalf of more individuals, perhaps increasing the chances that the claims will make it into court.

II. The Privacy Standing Problem

Courts are almost uniquely disinclined to recognize intangible harms in the area of privacy law. The legal standard for Article III standing is that a person must show "injury in fact" that is "concrete and particularized," as well as "actual or imminent," as outlined by the Supreme Court in *Lujan v. Defenders of Wildlife*.[10] These requirements sit particularly uncomfortably with information harms.[11] Information harms are certainly not "concrete" in the sense that they are tangible things one can hold in one's hand or easily measure in dollars. Courts appear to prefer harms that are "visceral and vested"—harms

9. Joshua Eaton, *Guardian Announces Leak of Classified NSA Documents*, Al Jazeera Am. (June 5, 2013), http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html.

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

11. *See generally* Seth F. Kreimer, *"Spooky Action at a Distance": Intangible Injury in Fact in the Information Age*, 18 U. Pa. J. Const. L. 745 (2016).

they can physically feel, that are measurable, and have already occurred.[12]

Similarly, information harms are rarely "particularized." They occur to millions of people, often in diffuse ways. Courts may worry that recognizing information harms will open the floodgates to litigation equivalent to taxpayer litigation: everybody who wants to might get into court. Information harms also often challenge the requirement that an injury be "actual or imminent." If we do not count information acquisition itself as harm, then any consequent economic effects of a breach might not be felt for years, yet plausibly could also occur at any instant.[13]

The hurdles to bringing claims for privacy harms are higher than in other areas of the law.[14] Courts regularly recognize intangible harms in cases with torts involving privacy, breach of confidence, and employment discrimination.[15] A wide variety of torts, ranging from assault to loss of consortium, serve to remedy "ethereal" emotional harms.[16] Courts have in other areas recognized that a significant risk of future harm may constitute a present harm.[17] Yet in the information privacy context, the Supreme Court and others have repeatedly asked for privacy plaintiffs to show something more.[18]

The Supreme Court most recently assessed privacy harm and Article III standing in *Spokeo Inc. v. Robins*.[19] In May 2016, an eight-member Supreme Court addressed in *Spokeo* whether the plaintiff (Robins) had standing to sue under the Fair Credit Reporting Act of 1970 (FCRA).[20] A six justice majority found that the Ninth Circuit had failed to properly evaluate Article III standing and remanded the case back to the Court of Appeals.[21]

---

12. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. (forthcoming 2017) (manuscript at 12), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885638; *see also* Daniel J. Solove, *Privacy and Data Security Violations: What's the Harm?*, LINKEDIN (June 25, 2014), https://www.linkedin.com/today/post/article/20140625045136-2259773-privacy-and-data-security-violations-what-s-the-harm.

13. Kreimer, *supra* note 11, at 774–75 (noting that "the penetrating qualities of the internet blur the line of "imminence").

14. Ryan Calo, *Privacy Harm Exceptionalism*, 12 J. TELECOMM. & HIGH TECH. L. 361–62 (2014); *see also* Citron & Solove, *supra* note 12 (manuscript at 23).

15. Citron & Solove, *supra* note 12 (manuscript at 23).

16. Calo, *supra* note 14 at 363; *see also* Citron & Solove, *supra* note 12 (manuscript at 23).

17. *Id.* (manuscript at 26) (citing Devlin v. Johns-Manville Corp., 495 A.2d 495, 561–62 (N.J. Super. Ct. Law Div. 1985) (recognizing a risk of cancer due to exposure to asbestos as present injury)).

18. *Devlin*, 495 A.2d at 503.

19. 136 S. Ct. 1540, 1544 (2016).

20. *Id*. at 1544.

21. *Id*. at 1550.

The Court explained that Article III injury in fact must be both particularized and concrete, and that while the Ninth Circuit had found particularized injury, it had not evaluated whether the injury was "concrete."[22] As to what constitutes "concrete" injury in the privacy context, the Court gave few guidelines. The majority explained that concrete injury need not be actually tangible; "intangible injuries can nevertheless be concrete."[23] To determine whether an intangible harm constitutes injury in fact, courts should look to both history and Congressional action as "instructive and important."[24] However, and confusingly, while Congress can sometimes legislate new injuries into existence, Congress cannot always legislate injury in fact into existence.[25] In particular, the court explained that "a bare procedural violation, divorced from any concrete harm," does not constitute an injury in fact.[26]

Thus according to the Court in *Spokeo*, Article III standing creates a Constitutional floor for Congress, though Congress can also somehow influence the floor by creating new rights. In some cases, violating a right granted by statute can be enough to constitute injury in fact, but in others, it appears courts will read in additional requirements.[27] How to line draw between these two is the exceedingly difficult question.

In *Spokeo*, the Court also nodded to an array of intangible yet concrete harms. The majority explained that a "risk of real harm" can satisfy the concreteness requirement, and that the law permits recovery by libel and slander victims even if those intangible harms are hard to measure.[28] Other Congressionally created information-related harms count, too, such as being unable to procure information through open government laws.[29]

---

22. *Id.* at 1545.

23. *Id.* at 1549.

24. *Id.*

25. *See Spokeo*, 136 S. Ct. at 1549 ("Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."); *see also id.* at 1547–48 (citing Raines v. Byrd, 521 U.S. 811, 820 ("Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing.")).

26. *Id.* at 1549.

27. *Id.* at 1549–50; *see also Sierra Club v. Morton*, 405 U.S. 727, 738 (1972) ("[B]roadening the categories of injury that may be alleged in support of standing is a different matter from abandoning the requirement that the party seeking review must himself have suffered an injury.").

28. *Spokeo*, 136 S. Ct. at 1549.

29. *Id.* (referring to the Federal Advisory Committee Act disclosure requirements and election disclosures).

With respect to FCRA, the statute at issue, the *Spokeo* majority clarified that it took no position as to whether Robins had adequately alleged an injury in fact.[30] The Court did, however, provide two FCRA-specific examples as guidance. A procedural violation of FCRA's notice requirement might not actually be harmful to a consumer, according to the majority, because the underlying information in the consumer profile might be "entirely accurate."[31] Similarly, the majority observed that "not all inaccuracies cause harm or present any material risk of harm."[32] The Court gave the example of an inaccurate zip code: "It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm."[33] Critics responded that an inaccurate zip code can certainly lead to concrete harm, such as being treated differently for credit purposes because you are from a predominantly African American neighborhood (a historic discriminatory practice known as "redlining").[34]

What are we to make of *Spokeo*? The decision puts off the more difficult questions for now. The truly thorny issues go back down to the Ninth Circuit, so that the Court—preferably one of nine members—can address them at a later time. At the same time, rather than requiring proof of economic or physical harms or threatened retaliation, the opinion acknowledges the adequacy of some intangible harms. The Court's references to libel, slander, and risk all suggest a broader view of privacy and standing than those advocated by the late Justice Scalia and discussed further below. On the other hand, the majority's very brief analysis of FCRA itself evinces skepticism of both notice requirements and accuracy requirements—features that are central to most privacy laws.[35]

Since *Spokeo*, several federal courts have dismissed information privacy claims for failure to assert a concrete injury in fact. A federal judge in the Southern District of Ohio found that job applicants at

30. *Id.* at 1550.

31. *Id.*

32. *Id.* at 1550.

33. *Id.*

34. G.S. Hans, Spokeo *Ruling Gives Few "Concrete" Answers on Privacy Rights*, CTR. DEMOCRACY & TECH. (May 17, 2016), https://cdt.org/blog/spokeo-ruling-gives-few-concrete-answers-on-privacy-rights/ ("ZIP codes, on their own, were used for redlining housing districts to keep out African-American families, which we would now consider a clear violation of individual rights.").

35. And to the Fair Information Practice Principles (FIPPs), established by the HEW and adopted by the OECD and countries around the world. *See generally* U.S. DEP'T OF HOMELAND SEC'Y, PRIVACY POLICY GUIDANCE MEMORANDUM (2008), https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

The Ohio State University had no standing to sue under FCRA.[36] At least three district courts have found that failing to comply with FCRA's (b)(1) certification requirement—which requires that companies requesting credit reports certify their compliance with FCRA — did not by itself give rise to a "concrete" injury under *Spokeo*.[37] A federal judge in Maryland remanded a class action against a hacked hospital to state court, reasoning that the hacking of patient information, such as names, addresses, dates of birth, and private health care information, did not rise to the level of concrete injury.[38] A federal judge in Wisconsin dismissed a class action against Time Warner Cable for an alleged violation of the Cable Communications Policy Act (CCPA), which requires the destruction of customers' personally identifiable information after it is no longer being used for the purpose for which it was collected.[39] The Eighth Circuit similarly found that a statutory violation of the "duty to destroy personally identifiable information by retaining certain information longer than the company should have kept it" failed to establish an injury in fact.[40] Several lower courts have found standing after *Spokeo*, looking to the two prongs of guidance identified by the Supreme Court: history and legislative action.[41] However, *Spokeo* has not overall provided more

36. *See* Smith v. Ohio State Univ., No. 15-CV-3030, 2016 WL 3182675, at *4 (S.D. Ohio June 8, 2016); *see also* Tyus, v. U.S. Postal Serv., No. 15-CV-1467, 2016 WL 6108942, at *6 (E.D. Wis. Oct. 19, 2016) (holding that inclusion of extraneous information on (b)(2) notice is not a "concrete" injury), *rev'd in part on other grounds on reh'g*, No. 15-CV-1467, 2017 WL 52609 (E.D. Wis. Jan. 4, 2017); Nokchan v. Lyft, Inc., No. 15-CV-03008 JCS, 2016 WL 5815287, at *9 (N.D. Cal. Oct. 5, 2016); Fisher v. Enter. Holdings, Inc., No. 4:15-CV-00372 AGF, 2016 WL 4665899, at *1 (E.D. Mo. Sept. 7, 2016).

37. *See* Larroque v. First Advantage LNS Screening Sols., Inc., No. 15-CV-04684-JSC, 2016 WL 4577257, at *5 (N.D. Cal. Sept. 2, 2016); Disalvo v. Intellicorp Records, Inc., No. 1:16-CV-1697, 2016 WL 5405258, at *3 (N.D. Ohio Sept. 27, 2016). *But see* Thomas v. FTS USA, LLC, No. 3:13-CV-825, 2016 WL 3653878, at *7 (E.D. Va. June 30, 2016) (finding that (b)(2) creates two rights which, when violated, each give rise to "concrete" injuries: (1) "a right to privacy in one's consumer report," and (2) "a right to specific information in the form of a clear and conspicuous" notice that one's consumer report would be released).

38. *See* Khan v. Children's Nat'l Health Sys., No. TDC-15-2125, 2016 WL 2946165, at *7 (D. Md. May 19, 2016).

39. *See* Gubala v. Time Warner Cable, Inc., No. 15-cv-1078-pp, 2016 WL 3390415, at *1 (E.D. Wis. June 17, 2016).

40. Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925, 930 (8th Cir. 2016); *see also* May v. Consumer Adjustment Co., No. 4:14-CV-166 HEA, 2017 WL 227964, at *3 (E.D. Mo. Jan. 19, 2017).

41. Perlin v. Time, No. 16-10635, 2017 WL 605291, at *12–13 (E.D. Mich. Feb. 15, 2017) (finding post-*Spokeo* that a violation of Michigan's video privacy act (VRPA) "is sufficient to satisfy the injury-in-fact requirement" and is "not a bare procedural violation"); *see also* Church v. Accretive Health, Inc., No. 15-15708, 2016 WL 3611543, at *3 (11th Cir. July 6, 2016) (applying *Spokeo* and holding that "through the [federal Fair Debt Collection Practices Act], Congress has created a new right—the right to receive [certain] required disclosures in communications governed by the [Act]—and a new injury—not receiving such disclosures."); *In re* Nickelodeon Con-

privacy protections; if anything, it has given lower courts more fodder for dismissing privacy claims. The Supreme Court has left intact the general sense of judicial skepticism over privacy injury.

Danielle Citron and Dan Solove recently proposed a framework for better evaluating privacy harms.[42] For data breach cases, they propose looking to the magnitude and likelihood of the potential harm, data sensitivity and data exposure, mitigating actions, and the reasonableness of preventative measures.[43] For other privacy violations, they propose less of a risk-based analysis and, instead, focus on what constitutes reasonable emotional distress.[44]

These proposed frameworks, however, still look for some kind of injury beyond the mere unapproved sharing of information.[45] What is striking about the national security cases following *Amnesty* and discussed at length below is that many find standing solely because information has been shared without permission. This is consistent with at least two post-*Spokeo* cases finding that unauthorized disclosure alone may constitute injury in fact.[46]

III. Standing After Snowden

What counts as a privacy harm? Surprisingly, recent national security litigation may yield answers that are friendlier to privacy than data breach litigation has been. In the wake of Snowden's revelations of the extent of U.S. national security surveillance, courts have had to evaluate what plaintiffs must show to articulate Article III injury in fact. The ensuing cases yield lessons about privacy and injury in fact.

A. Clapper v. Amnesty International *and the Snowden Leaks*

The leading case on standing and national security surveillance is the much misunderstood *Clapper v. Amnesty International*,[47] decided by the Supreme Court in February 2013. The *Amnesty* plaintiffs

sumer Privacy Litig., No. 15-1441, 2016 WL 3513782, at *7 (3d Cir. June 27, 2016) (holding that disclosure of information in violation of the federal Video Privacy Protection Act resulted in a concrete harm "in the sense that it involve[d] a clear *de facto* injury, *i.e.*, the unlawful disclosure of legally protected information.").

42. Citron & Solove, *supra* note 12 (manuscript at 5).

43. *Id.* at 28–29.

44. *Id.* at 30–31.

45. *Id.* at 10 (explaining that courts have generally refused to recognize harm in circumstances when data is shared with other companies without permission). The Court then proposes the risk-based multi-part framework for evaluating when privacy harm occurs in data breaches. *Id.* at 42–44.

46. *See Perlin*, 2017 WL 605291, at *12; *In re* Nickelodeon Consumer Privacy Litig., No. 15-1441, 2016 WL 3513782, at *7 (3d Cir. June 27, 2016).

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

facially challenged Section 702 of the FISA Amendments Act on the day the statute was enacted.[48] Because this was a facial challenge, and because the government kept the extent of its surveillance programs largely secret, the Court observed that "respondents fail to offer any evidence" of actual government surveillance and "have no actual knowledge" of any surveillance programs under Section 702.[49] Characterizing the plaintiffs' claim that they would be subject to surveillance as "highly speculative," the Court refused under those circumstances to find standing.[50]

Then in June 2013, a mere four months after *Amnesty*, the Snowden stories began. First, *The Guardian* revealed the government's program for gathering phone subscriber metadata (that is, phone numbers dialed, among other things) under Section 215 of the Patriot Act.[51] Then both *The Guardian* and *The Washington Post* revealed that the U.S. government was obtaining communications content directly from communications providers under its Section 702 authority through a program called PRISM.[52] Subsequent news stories revealed that the government was conducting backbone surveillance through the fiber-optic cables of service providers like Google,[53] targeting encrypted content,[54] gathering content directly through communications infrastructure using "Upstream" surveillance,[55] and much more.

The challenge in *Amnesty* was that plaintiffs could not show they had in fact been surveilled for purposes of standing, because they had no actual knowledge of the existence of any government surveillance programs arising under the statute. They had no actual knowledge of

48. *Id*. at 1146.

49. *Id.* at 1148.

50. *Id.*

51. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. *See generally* Joshua Eaton, *Timeline of Edward Snowden's Revelations*, AL JAZEERA AM., http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html (last visited Aug. 8, 2016).

52. Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers; Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013, 3:23 PM), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

53. Nicole Perlroth & John Markoff, *N.S.A May Have Hit Internet Companies at a Weak Spot*, N.Y. TIMES (Nov. 25, 2013), http://www.nytimes.com/2013/11/26/technology/a-peephole-for-the-nsa.html?pagewanted=all&_r=0.

54. Jake Appelbaum et al., *NSA Targets the Privacy-Conscious*, DAS ERSTE (July 3, 2014, 5:08 PM), http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html.

55. Craig Timberg, *NSA Slide Shows Surveillance of Undersea Cables*, WASH. POST (July 10, 2013), https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html.

these government surveillance programs because the programs were kept secret by the plaintiffs' adversary—the government. After the Snowden leaks, that changed.[56] As Snowden asked American Civil Liberties Union attorney Ben Wizner in their first online conversation: "Do you have standing now?"[57]

B. Standing After Snowden

Amnesty is now often cited for the proposition that injury must be "certainly impending" to constitute injury in fact,[58] but what this means has been misunderstood by lower courts.[59] In *Amnesty*, the Court described five links in a "highly attenuated chain of possibilities" that compounded together did "not satisfy the requirement that threatened injury must be certainly impending."[60] In other words, the plaintiffs could not show that government surveillance itself was certainly impending—the Court, in its assessment of standing in *Amnesty*, was not referring to a requirement of additional tangible economic or physical harms. Subsequent cases have misunderstood *Amnesty* to require that in addition to the unauthorized appropriation of information, privacy and data breach plaintiffs must show other certainly impending harms.[61]

Two of the links in *Amnesty*'s "highly attenuated chain of possibilities" were broken by the Snowden stories. The Court did not at the time of *Amnesty* know what surveillance programs existed under Section 702 or the extent to which the FISA Court had authorized or restricted these programs. After Snowden, the plaintiffs knew both. In fact, after Snowden, some plaintiffs knew even more: They themselves were definitely the subjects of metadata surveillance.

1. Interception of Communications Content Alone Can Be Injury in Fact

The Court made an important point in *Amnesty* that has been often overlooked. The majority and dissent agreed that if a plaintiff could

56. *But see* Stephen I. Vladeck, *Standing and Secret Surveillance*, 10 I/S J.L. & POL'Y FOR INFO. SOC'Y 551, 553 (2014) ("[A]lthough these disclosures seem to give even greater credence to the plaintiffs' allegations in *Clapper*, they don't necessarily cure the standing defect identified by Justice Alito.").

57. Kashmir Hill, *How ACLU Attorney Ben Wizner Became Snowden's Lawyer*, FORBES (Mar. 10, 2014, 4:27 PM), http://www.forbes.com/sites/kashmirhill/2014/03/10/how-aclu-attorney-ben-wizner-became-snowdens-lawyer/.

58. *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 651 (S.D. Ohio 2014).

59. Kreimer, *supra* note 11, at 766.

60. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148 (2013).

61. Kreimer, *supra* note 11, at 765 n.70.

show actual interception of the content of communications, then the plaintiff would have Article III standing.[62] Justice Breyer, writing for the dissent, observed that "[n]o one here denies that the Government's interception of a private telephone or e-mail conversation amounts to an injury that is 'concrete and particularized.'"[63] Justice Alito, writing for the majority, appeared to agree.[64]

One of the lessons from national security surveillance litigation, then, is that the interception of communications by an unintended third party can constitute injury in fact.[65] Courts citing *Amnesty* in data breach cases often cite it for the proposition that a plaintiff must show "certainly impending" harm beyond the illicit breach itself, such as economic harm.[66] That characterization of *Amnesty* is incorrect. If anything, *Amnesty* suggests that when communications content is hacked by a third-party (in that case, the government), the interception alone constitutes injury in fact.

2. *Seizure and Maintenance of a Database of Nonsensitive Information Can Be Injury in Fact*

Many data breach and data privacy lawsuits do not involve wiretapping or hacking the contents of private communications. They tend, instead, to involve the seizure of data points about individuals. For example, plaintiffs in a class action sued Urban Outfitters and Anthropologie over the collection of customer zip codes—precisely the kind of information the Supreme Court suggested is inherently not harmful in *Spokeo*.[67] Can the bulk gathering of individually nonsensitive data points create privacy harms? Again, post-Snowden national security surveillance case law is illuminating. In several cases since the Snowden revelations, lower courts have had to determine whether government seizure of customer call records gives rise to standing under Article III. Courts have said that the seizure of these records, with nothing more, is enough to demonstrate injury in fact. This sug-

62. *Id*. at 1156.

63. *Id.* at 1155 (Breyer, J., dissenting).

64. *Id.* at 1153 (explaining that the case would look like Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167 (2000), and Meese v. Keene, 481 U.S. 465 (1987), in which plaintiffs would have standing if, on remand, they could show actual acquisition of content information).

65. Kreimer, *supra* note 11, at 759.

66. *Id.* at 765 n.70 (listing several cases that cite this proposition).

67. Brandon Lowrey, *Urban Outfitters ZIP Code Class Says It Can Pass* Spokeo *Test*, Law360 (June 24, 2016, 11:09 AM), http://www.law360.com/articles/811008/urban-outfitters-zip-code-class-says-it-can-pass-spokeo-test.

gests that the bulk collection of nonsensitive information and storage in a database can itself be harm, without additional showings.

In 2015, the Second Circuit determined in *ACLU v. Clapper*[68] that government seizure of Verizon Business call records gave rise to injury in fact for a Fourth Amendment claim.[69] The government had asked the court to require an additional showing by the plaintiffs that the phone numbers would be included in the results of government queries of the database of call records or would be used as search terms in querying the database.[70] In other words, the government asked for proof not only that it had acquired the records, but that it was using them in a harmful way. This would likely have been impossible to do because of national security secrecy.

The Second Circuit denied the government's request for a further showing of harm beyond the collection of the records. The court explained, "[w]hether or not such claims prevail on the merits, appellants surely have standing to allege injury from the collection, and maintenance in a government database, of records relating to them."[71] The seizure and maintenance of the call record information was enough to give rise to injury in fact.

The D.C. Circuit Court of Appeals has also addressed standing to sue the government for metadata surveillance, and thus addressed this question of how to handle nonsensitive information collected and stored in bulk.[72] In a per curiam opinion, the panel vacated the district court's grant of a preliminary injunction to the plaintiffs.[73] The judges disagreed on whether the plaintiffs needed to definitively show that they had themselves been subjected to government surveillance versus showing a strong inference that they had been subjected to the surveillance program. Writing individually, Judge Brown addressed the issue of standing. Judge Brown explained that while the plaintiffs had shown only a possibility that their own call records were collected, they had successfully shown that the government operates a bulk-telephony metadata program collecting subscriber information and could thus show an inference that their specific records had been collected.[74] This, in his opinion, would be enough to satisfy the "bare requirements of standing."[75] Judge Williams, writing individually, dis-

68. ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).
69. *Id*. at 801.
70. *Id.*
71. *Id.* at 801.
72. Obama v. Klayman, 800 F.3d 559, 560–62 (D.C. Cir. 2015) (per curiam).
73. *Id.* at 562
74. *Id.*
75. *Id.* at 562–64.

agreed. He explained that he would not have found standing, because the plaintiffs were not subscribers of Verizon Business Network Services, "the sole provider that the government has acknowledged targeting for bulk collection."[76] Crucially, both judges, however, agreed that if the plaintiffs could show that "records involving their calls have actually been collected," then they would have standing to sue.[77] Thus two panelists on the D.C. Circuit Court of Appeals in fact agreed with the Second Circuit's conclusion that collection of metadata conveys standing.

These cases conclude that the seizure of call record information by the government by itself gives rise to standing, without the need to show additional economic or more tangible harms. These holdings are particularly striking because call record information, a type of "metadata," has repeatedly been referred to in Fourth Amendment caselaw as nonsensitive information.[78] If the seizure and holding of metadata can give rise to injury in fact, the bulk seizure and storage of more sensitive information should get a plaintiff into court.

3. The "Chilling Effect" and Standing

National security surveillance cases have been the site of important discussions of when a "chilling effect" can give rise to standing. The chilling effect is a classic, well-recognized First Amendment injury, which occurs when an individual self-censors in response to government action.[79] The Fourth Circuit, for example, has held that the chilling effect is injury in fact for purposes of asserting a First Amendment claim, so long as the self-censorship is objectively reasonable.[80] Requiring a showing of an objectively reasonable chilling effect could be a compromise between requiring no showing of harm apart from data seizure on the one hand, and recognizing only showings of economic or physical harm on the other.

In practice, however, whether the chilling effect can be asserted as injury in fact in surveillance cases is a challenging question. In *Am-*

---

76. *Id.* at 565.

77. *Id.*

78. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 745-46 (1979).

79. *See, e.g.*, Cooksey v. Futrell, 721 F.3d 226, 235 (4th Cir. 2013) ("In First Amendment cases, the injury-in-fact element is commonly satisfied by a sufficient showing of 'self-censorship, which occurs when a claimant is chilled from exercising h[is] right to free expression.'" (quoting Benham v. City of Charlotte, 635 F.3d 129, 135 (4th Cir. 2011))).

80. *Benham*, 635 F.3d at 135. A chilling effect may constitute injury in fact if the government action is "likely to deter a person of ordinary firmness from the exercise of First Amendment rights." *Id*. (quoting Constantine v. Rectors & Visitors of George Mason Univ., 411 F.3d 474, 500 (4th Cir. 2005)).

nesty, one of the harms asserted by the plaintiffs was that attorneys could not speak freely with their clients because they feared surveillance, and had altered their behavior by refraining from speaking openly or at all.[81] The Court rejected this approach, holding that absent a more plausible showing that the surveillance programs actually existed and applied to the plaintiffs, self-inflicted harms were not enough to give rise to standing.[82]

But *Amnesty* does not answer whether a plausible chilling effect will ever be adequate to convey standing. One way of understanding *Amnesty*'s reasoning about the chilling effect is that the plaintiffs' self-censoring behavior was not in fact reasonable in that case because the plaintiffs had not plausibly shown that a surveillance program in fact existed or that they themselves were subject to it.[83] The other way to understand *Amnesty*, however, is the way the late Justice Scalia would have liked to characterize chilling effects: Chilling effects alone are not enough to convey standing, absent a further showing of coercive or punitive government action. *Amnesty*'s discussion of chilling effects is a window onto this larger debate.

Justice Scalia was generally skeptical of intangible injuries.[84] This skepticism was even more visible in the privacy context. The majority's skepticism of chilling effects in *Amnesty* echoes a theme from Justice Scalia's jurisprudence: Privacy harm is not real unless some other bad thing happens.[85]

How the rest of the Supreme Court Justices feels about this is unclear. Relatively recent Court cases recognize privacy rights stemming from the First Amendment's protections of both speech and association.[86] Justice Scalia believed that merely requiring an individual to reveal her identity was not enough to show a First Amendment harm;

---

81. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1152 (2013).

82. *Id.* at 1152–53.

83. *See id.* at 1151 (characterizing the Second Circuit holding as evaluating the plaintiffs' harm under a "relaxed reasonableness" standard, and observing that "respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending").

84. *See* Kreimer, *supra* note 11, at 751 ("Justice Scalia and his acolytes take the position that Article III doctrine requires a tough minded, common sense and practical approach. Injuries in fact should be 'tangible,' 'direct,' 'concrete,' 'de facto,' realities . . . ."); *see also* Stephen I. Vladeck, *Standing After Scalia* (Sept. 2, 2016) (unpublished manuscript), https://administrativestate.gmu.edu/wp-content/uploads/sites/29/2017/04/Standing-After-Scalia.pdf.

85. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1149 (2013). The majority cites Justice Scalia's decision about chilling effects and surveillance from when he was a Court of Appeals judge on the D.C. Circuit. *Id.*

86. *See, e.g.*, Doe v. Reed, 561 U.S. 186, 191 (2010); Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Village of Stratton, 536 U.S. 150, 153 (2002); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 336 (1995); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 460 (1958).

the individual also, according to Justice Scalia, should have to show evidence of possible retaliation against her for her speech.[87] In a series of cases, the majority of the Court did not agree, and found that when the government requires a person to identify herself as a speaker, in writing, that coercion alone can constitute a First Amendment harm, with no additional evidence of retaliation needed.[88]

Whether a subjective chilling effect can constitute injury in fact for purposes of challenging surveillance is less clear. The late Justice Scalia's views on the matter are again apparent. While sitting on the D.C. Circuit, then-Judge Scalia wrote in *United Presbyterian Church in the U.S.A. v. Reagan*[89] that plaintiffs who asserted a "chilling effect" did not have standing to challenge government surveillance under an Executive Order.[90] Sounding similar to courts in data breach cases who look for visceral and vested harms, then-Judge Scalia explained that the "harm of 'chilling effect' is to be distinguished from the immediate threat of concrete, harmful [government] action."[91] Justice Scalia claimed that such an avenue to standing had been foreclosed by an earlier Supreme Court case, *Laird v. Tatum*.[92] He cited *Laird* for the proposition that "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm."[93]

In *Amnesty*, the majority cited Justice Scalia's opinion in *United Presbyterian*, among other cases, for the proposition that one cannot achieve standing solely by invoking a "chilling effect" produced by a subjective fear of being subjected to illegal government surveillance.[94] However, *Amnesty* is fact-bound and not the last word. The Court was largely concerned that the plaintiffs had failed to show the very existence of a surveillance program under the challenged statute. In the absence of that showing, plaintiffs clearly could not show that they themselves were subject to surveillance and thus could not assert a legitimate chilling effect.[95] *Amnesty* does not foreclose recognition of the chilling effect for purposes of finding standing when a surveillance program has clearly been shown to exist and applies to the plaintiffs.

87. *McIntyre*, 514 U.S. at 379 (Scalia, J., dissenting).
88. *Id.* at 353.
89. 738 F.2d 1375 (D.C. Cir. 1984).
90. *Id*. at 1380.
91. *Id.*
92. 408 U.S. 1 (1972).
93. *United Presbyterian*, 738 F.2d at 1378 (quoting *Laird*, 408 U.S. at 13–14).
94. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1152 (2013).
95. *Id.* at 1149, 1152–53 (listing the cases arising out of Laird, and concluding that "respondents' self-inflicted injuries are not fairly traceable to the Government's purported activities under § 1881a, and their subjective fear of surveillance does not give rise to standing").

The earlier case, *Laird v. Tatum*, also does not foreclose a finding of standing based on chilling effects arising from illicitly surveilling private communications, uncovering speakers' hidden identities, or uncovering private associations.[96] The Court in *Laird* did not address illicit or illegal surveillance, but instead addressed the Army's otherwise legal surveillance of individuals in public. As characterized two years later by Justice Marshall, *Laird* stands primarily for the need for specific, rather than general, allegations of a chilling effect.[97] While Justice Scalia hinged his call for tangible injury on *Laird*'s language requiring the government to not just surveil behavior but affirmatively proscribe it,[98] Justice Marshall characterized that language as dicta.[99]

This all leaves the chilling effect in a nebulous place. On the one hand, it is a well-recognized First Amendment injury, and the Supreme Court has recognized that forcing a person to identify herself gets that person into court without any need to show subsequent, more "tangible" harms. On the other hand, *Amnesty* suggests that it will be difficult to use the chilling effect alone to achieve standing to challenge privacy harms. It would be wrong to read *Amnesty* and *Laird* to foreclose the use of specific allegations of chilling effects to achieve standing. I, along with others, have argued this in a recent amicus brief in the Fourth Circuit, for an ongoing case challenging "Upstream" surveillance of the content of internet communications under Section 702.[100]

In the data breach context, it is unclear how this would play out. As discussed below, there are no First Amendment claims against private actors. However, if Congress should decide to grant standing in a stat-

96. *Laird*, 408 U.S. at 9, 11 (noting that there was "no evidence of illegal or unlawful surveillance activities" (quoting Tatum v. Laird, 444 F.2d 947, 953 (D.C. Cir. 1971))).

97. *See* Socialist Workers Party v. Attorney Gen., 419 U.S. 1314, 1319 (1974) ("In this case, the allegations are much more specific: the applicants have complained that the challenged investigative activity will have the concrete effects of dissuading some YSA delegates from participating actively in the convention and leading to possible loss of employment for those who are identified as being in attendance. Whether the claimed 'chill' is substantial or not is still subject to question, but . . . [t]he specificity of the injury claimed . . . is sufficient, under *Laird*, to satisfy the requirements of Art. III.").

98. *See United Presbyterian*, 738 F.2d at 1378 ("[I]n each of these cases, the challenged exercise of governmental power was regulatory, proscriptive, or compulsory in nature, and the complainant was either presently or prospectively subject to the regulations, proscriptions, or compulsions that he was challenging." (alteration in original) (quoting *Laird*, 408 U.S. at 11)).

99. *Socialist Workers Party*, 419 U.S. at 1318 (characterizing the discussion in *Laird* of regulatory, proscriptive, or compulsory exercises of government power as dicta "merely distinguishing earlier cases, not setting out a rule for determining whether an action is justiciable or not").

100. Brief of Amicus Curiae First Amendment Legal Scholars in Support of Plaintiffs-Appellants and Supporting Reversal at 11, Wikimedia Found. v. NSA, 143 F. Supp. 3d 344 (4th Cir. 2016) (No. 15-2560), 2015 WL 13016204.

ute based on harms that look like the chilling effect, one could argue that similar assertions of chilling effects from an actual data breach or illicit collection of information could be enough to satisfy Article III's requirements.

4. Other Gleanings About Data Harms

The national security surveillance case law is worth perusing for a fourth reason: Apart from the decisions on standing specifically, these cases contain interesting and complex analyses of privacy harms. These analyses are more nuanced and more comprehending of the implications of Big Data than much of the judicial reasoning in the private data breach context.

This nuance reflects recent shifts by the Supreme Court in Fourth Amendment case law. The Court recently appears to be more willing to recognize the privacy harms associated with Big Data. In *United States v. Jones*,[101] for example, five justices noted that tracking an individual over twenty-eight days could give rise to significant privacy harms by creating a complex portrait of that individual through the accumulation and analysis of individual data points, and inferences derived from them.[102] Location data "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[103]

In *Riley v. California*,[104] the majority of the court (eight justices—including Justice Scalia) found that searching an individual's cell phone caused cognizable privacy harms because of the vast amount of data contained therein.[105] The Court observed that

> a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet.[106]

In national security surveillance litigation, few courts have addressed these types of privacy harms—in part because most of the litigation is early stage or is now moot after passage of the U.S.A. Freedom Act changing the government's phone records collection

101. 565 U.S. 400 (2011).
102. *Id*. at 412–13.
103. *Id.* at 414–15 (Sotomayor, J., concurring).
104. 134 S. Ct. 2473 (2014).
105. *Id*. at 2485.
106. *Id*. at 2489.

program.[107] The cases that have addressed the harm arising from large databases, however, have been notable.

Writing after *Jones* but before *Riley*, Judge Leon of the District Court for the District of Columbia explained that with the sheer quantity of data now available to the government, seizure of even ordinarily nonsensitive information now provides "an entire mosaic—a vibrant and constantly updating picture of the person's life."[108] Similarly, the Second Circuit, while declining to reach the Constitutional questions, sympathetically characterized the appellants' argument as follows: "the bulk collection of data as to essentially the entire population of the United States, something inconceivable before the advent of high-speed computers, permits the development of a government database with a potential for invasions of privacy unimaginable in the past."[109] The court explained that while it decided the case on statutory rather than Constitutional grounds, "[t]he seriousness of the constitutional concerns . . . has some bearing on what we hold today . . . ."[110]

Digital privacy has long been subjected to the much-bemoaned third-party doctrine: The idea that once a person voluntarily shares information with another, she relinquishes a privacy interest in that information.[111] This gremlin has raised its head in similar forms in private sector litigation as well, with courts reading privacy statutes not to apply to third parties because individuals voluntarily shared the information with websites.[112] FTC privacy enforcement, by contrast, is triggered precisely because a person has shared their information with a company, highlighting how ill-suited the third-party doctrine is to the digital age.[113] But recent case law suggests that courts are beginning to understand that vast quantities of data make a difference, turning nonsensitive information into sensitive information through readily-made inferences, and suggesting that privacy interests remain, even when we entrust that information to third parties.[114]

---

107. *See, e.g.*, ACLU v. Clapper, 785 F.3d 787, 825 (2d Cir. 2015).

108. Klayman v. Obama, 957 F. Supp. 2d 1, 36 (D.C. Cir. 2013), *vacated*, 800 F.3d 559 (D.C. Cir. 2015).

109. *Clapper*, 785 F.3d at 824.

110. *Id.*

111. *See* United States v. Miller, 425 U.S. 435, 443 (1976); *see also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979). Another important component of this doctrine, however, is that the information shared is usually not sensitive.

112. *See, e.g.*, *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

113. Margot E. Kaminski, *Robots in the Home: What Will We Have Agreed To?*, 51 IDAHO L. REV. 661, 674–75 (2015).

114. United States v. Jones, 565 U.S. 400 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy

5. Summary of Standing Lessons After Snowden

In summary, recent national security surveillance litigation may yield lessons for discussions of standing in the data breach context. First, if the hacked or breached information contains the content of private communications, that breach alone may be cognizable injury in fact. Second, even if the information illicitly gathered is less sensitive information, if it is gathered in large enough quantities and maintained in a database for analysis, that too should be a cognizable harm. Third, the assertion of a specific, nonsubjective chilling effect due to a breach or interception could be a harm. Fourth and finally, courts in the national security and Fourth Amendment contexts appear more ready to recognize that profiling based on Big Data can itself be a privacy harm.

6. Caveats

There are, of course, important differences between data breach litigation and First and Fourth Amendment litigation. In First and Fourth Amendment cases, the government is the illicit actor, and in both contexts, the government has enforcement and coercion powers that private actors presumably do not. Perhaps for this reason—the lack of a governmental Sword of Damocles—one could justify looking for some additional more tangible, impending harm when private data breaches occur. But courts do not bother to explain this; most just assume without discussion that additional harm beyond illicit data acquisition must be shown. And most courts readily draw on *Amnesty*'s standing analysis in the private sector context without distinguishing between government and private sector behavior.

Another way to distinguish the data breach context is that the party being sued is usually not the hacker, but the database holder. Perhaps plaintiffs should have an easier time going after the perpetrator of an illicit acquisition than after the hacked party housing the data. This distinction seems, however, more appropriately made in discussions of how fairly traceable the injury is to a defendant's actions, not in discussions of whether the underlying injury constitutes injury in fact. Congress can certainly decide either not to bestow statutory standing or to create additional hurdles to obtaining damages against a defendant who carelessly housed the data. The question is whether courts can, using Article III, obviate Congress' decisions on when to give

---

in information voluntarily disclosed to third parties" because that "approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.").

plaintiffs standing to sue. As Felix Wu points out in his contribution to the *22nd Annual Clifford Symposium on Tort Law and Social Policy*, courts' recent willingness to use Article III standing inquiries to undermine legislative decisions on data harms seems to fly in the face of the separation-of-powers justification for using Article III to restrict federal courts' powers to begin with.[115]

IV. Corporate Responsibility and the Security State

Because the *22nd Annual Clifford Symposium* is not just about data theft, but also about corporate responsibility, I would be remiss if I did not close by discussing corporate responsibility in light of national security surveillance.

Corporations entrusted with consumer data stand to lose, and have lost, enormous amounts of money when they lose consumer trust.[116] Consumer trust includes trust that information will not be turned over to the government wholesale. Since the Snowden leaks, companies have seen global losses on an enormous scale.[117] The recent collapse of the E.U.-U.S. Safe Harbor agreement in the European Court of Justice's *Schrems* decision cemented the global economic impact of national security surveillance.[118] The replacement agreement between the E.U. and U.S.—the Privacy Shield—has been challenged in Ireland on similar grounds, and could similarly disrupt digital trade.[119]

In 2014, Forrester Research, a technology research firm, predicted that data security and privacy would be competitive differentiators in 2015.[120] If the Apple-FBI debacle and recent WhatsApp encryption

115. *See* Felix Wu, *How Privacy Distorted Standing Law*, 66 DePaul L. Rev. 439 (2017) (manuscript at 2); *see also* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) ("[th]e law of Article III standing . . . serves to prevent the judicial process from being used to usurp the powers of the political branches" (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1146 (2013))).

116. Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. Times (Mar. 21, 2014), https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0%20.

117. *Id*. (indicating global losses as high as $180 billion).

118. Natasha Lomas, *Europe's Top Court Strikes Down 'Safe Harbor' Data-Transfer Agreement with U.S.*, TechCrunch (Oct. 6, 2015), http://techcrunch.com/2015/10/06/europes-top-court-strikes-down-safe-harbor-data-transfer-agreement-with-u-s/; *see also* Lisa Mays & Scott Maberry, *The Schrems Decision: How the End of Safe Harbor Affects Your FCPA Compliance Plan*, Global Trade L. Blog (Nov. 12, 2015), http://www.globaltradelawblog.com/2015/11/12/the-schrems-decision-how-the-end-of-safe-harbor-affects-your-fcpa-compliance-plan/.

119. Karlin Lillington, *Court Challenge to Privacy Shield Will Have Wide Reverberations*, Irish Times (Nov. 3, 2016), http://www.irishtimes.com/business/technology/court-challenge-to-privacy-shield-will-have-wide-reverberations-1.2852231.

120. Heidi Shey et al., *Predictions 2015: Data Security and Privacy Are Competitive Differentiators*, Forrester (Nov. 12, 2014), https://www.forrester.com/report/Predictions+2015‡ata+Security+And+Privacy+Are+Competitive‡ifferentiators/-/E-RES116328.

are any indicators, this is correct.[121] Installing security that protects consumers against government surveillance is only part of the battle, however.

This Article closes by suggesting that corporations should take up the mantle of challenging national security surveillance.[122] Not only do they have the deeper pockets to do so more effectively, but they have two additional advantages related to standing that suggest they are in the best position to challenge these programs. First, corporations have informational advantages; they often know when the government is asking to obtain user information, when users do not. Second, because corporations have many users, they are better positioned to overcome the *Amnesty* "certainly impending" hurdle to probabilistically show the likelihood that any one of their users is definitely being scrutinized.

A. Challenging Substantive Law

Corporations can challenge the substantive law that enables government surveillance. Corporations are both better equipped to challenge this surveillance because of deeper financial resources, and are capable of challenging the surveillance of their customers even when those users do not know they are being surveilled, or are otherwise unable to bring claims themselves. Recently, we have seen several companies engaging in this kind of policy litigation around surveillance.

In 2016, Apple famously refused to unlock the iPhone of deceased San Bernadino gunman Syed Rizwan Farook in response to the FBI's request.[123] Apple CEO Tim Cook explained that the FBI's request not only threatened cybersecurity, but threatened user privacy, because smartphones are used "to store an incredible amount of personal information, from our private conversations to our photos, our music, our notes . . . our financial information and health data, even where we have been and where we are going."[124] While Apple liti-

121. Cade Metz, *Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People*, WIRED (Apr. 5, 2016, 11:00 AM), http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/.

122. For a longer and more general discussion of the roles of private actors in shaping the "surveillance executive," see Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. (forthcoming 2018).

123. Elizabeth Weise, *Apple v FBI Timeline: 43 Days that Rocked Tech*, USA TODAY (Mar. 30, 2016, 10:46 AM), http://www.usatoday.com/story/tech/news/2016/03/15/apple-v-fbi-timeline/81827400/.

124. Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016) http://www.apple.com/customer-letter/.

gated the case, with two groups of a total of thirty-two technology companies filing in support, the FBI eventually withdrew its legal action.[125]

In 2015, Microsoft argued that it should not have to produce the contents of an email account stored on a server located outside of the United States.[126] The Second Circuit decided for Microsoft.[127] This left the U.S. government to use more "cumbersome" methods outlined in international agreements with other countries if it wanted to obtain the emails.[128] Scholars dispute the value of this holding for privacy. On the one hand, it is a win by a technology company against a government request for customer emails. Numerous public interest groups supported Microsoft's appeal with amicus briefs.[129] The case is also a win for individual country sovereignty, for those countries that wish to protect privacy more than it is protected in the United States.[130] On the other hand, the case holds that U.S. privacy law does not apply abroad, so if U.S. law is better than the privacy standards of a particular country, the case could be a loss for privacy.[131]

Both the Apple-FBI challenge and the Microsoft challenge point to an increasing willingness on the part of companies to substantively challenge surveillance law on behalf of their users. Other companies have also joined the fray. Yahoo challenged foreign-intelligence surveillance in the FISA court.[132] Facebook challenged a sealed bulk

125. Kif Leswing, *Apple Won Its Battle Against the FBI, But the War Isn't Over Yet*, BUS. INSIDER (Mar. 30, 2016), http://www.businessinsider.com/apple-won-fbi-battle-but-the-war-isnt-over-2016-3.

126. *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 200–01 (2d Cir. 2016).

127. *Id.* at 220 ("[E]xecution of the Warrant would constitute an unlawful extraterritorial application of the Act.").

128. *Id.* at 221 ("[T]he current process for obtaining foreign-stored data is cumbersome. That process is governed by a series of Mutual Legal Assistance Treaties ("MLATs") between the United States and other countries, which allow signatory states to request one another's assistance with ongoing criminal investigations, including issuance and execution of search warrants.").

129. *In re* Warrant to Search a Certain E-Mail, 829 F.3d at 199. The ACLU, the Constitution Project, and the Electronic Frontier Foundation filed an amicus brief siding with Microsoft; so did the Center for Democracy and Technology.

130. *See, e.g.*, Daniel Solove, *Microsoft Just Won a Big Victory Against Government Surveillance—Why It Matters*, LINKEDIN (Jul. 15, 2016), https://www.linkedin.com/pulse/microsoft-just-won-big-victory-against-government-why-daniel-solove?articleId=6159558655122427905#comments-6159558655122427905&trk=prof-post; *see also @jreidenberg*, TWITTER (Jul. 14, 2016, 8:41 AM), https://twitter.com/jreidenberg/status/753615536043520000.

131. Andrew Keane Woods, *Reactions to the Microsoft Warrant Case*, LAWFARE (Jul. 15, 2016, 7:21 AM), https://www.lawfareblog.com/reactions-microsoft-warrant-case.

132. *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1008–09 (FISA Ct. Rev. 2008).

search warrant for 381 user accounts.[133] This is likely in the companies' business interests, as users purportedly shop for companies who provide data security and withstand government surveillance.[134] As skeptics point out, however, corporate challenges to government requests for users' data have been few and far between, because of longstanding structural alliances between government and communications companies.[135] It "may be too early to tell" whether the post-Snowden market will continue to encourage these types of litigation.[136]

B. Challenging National Security Letters and Gag Orders

In the wake of Snowden, companies have also challenged their inability to communicate with the public about the extent of government surveillance. Numerous statutes prevent communications companies from disclosing surveillance orders to the public or to those being surveilled.[137] Recently, companies have challenged these gag orders as restrictions on their freedom of speech.

In early days after the Snowden leaks, Facebook, Yahoo, and Microsoft won permission to include FISA requests in their releases of the overall number of court orders received.[138] Google asked the Foreign Intelligence Surveillance Court to ease its gag order, citing First Amendment concerns.[139] In October 2014, Twitter sued the government, challenging its inability to disclose the number of surveillance requests it receives.[140] In May 2016, a federal judge dismissed

133. *In re* 381 Search Warrants Directed to Facebook, Inc., 14 N.Y.S.3d 23 (App. Div. 2015); James C. McKinley Jr., *Court Weighs Facebook's Right to Challenge Search Warrants on Users' Behalf*, N.Y. TIMES (Dec. 11, 2014), http://www.nytimes.com/2014/12/12/nyregion/courtweighs-facebooks-right-to-challenge-search-warrants-on-users-behalf.html.

134. Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 IOWA L. REV. 1441, 1481–82 (2015) (describing increased corporate response to government surveillance, post-Snowden, in reaction to market forces).

135. *Id.* at 1473 ("The government and tech companies enjoy a close, interdependent relationship that is highly beneficial to both sectors.").

136. *Id.* at 1484.

137. *See 11-Year Legal Battle Ends with Clinic Victory*, YALE L. SCH. (Nov. 30, 2015), https://www.law.yale.edu/yls-today/news/11-year-legal-battle-ends-clinic-victory; *see also* 18 U.S.C. §§ 2513, 2515 (2012).

138. Craig Timberg & Cecilia Kang, *Google Challenges U.S. Gag Order, Citing First Amendment*, WASH. POST (June 18, 2013), https://www.washingtonpost.com/business/technology/google-challenges-us-gag-order-citing-first-amendment/2013/06/18/96835c72-d832-11e2-a9f2-42ee3912ae0e_story.html.

139. *Id.*

140. Ben Lee, *Taking the Fight for #transparency to Court*, TWITTER BLOG (Oct. 7, 2014, 5:19 PM), https://blog.twitter.com/2014/taking-the-fight-for-transparency-to-court (describing Twitter's First Amendment challenge to restrictions on disclosure of the number of national security letters, or NSLs, and Foreign Intelligence Surveillance ACT (FISA) court orders received).

the case, explaining that Twitter had failed to challenge underlying classification decisions.[141] Litigation in the Twitter case is ongoing.[142]

Limited success in the national security realm has not stopped companies from challenging gag orders in other areas of surveillance law. In 2015, Yahoo successfully challenged a gag order indefinitely prohibiting it from disclosing a grand jury subpoena seeking subscriber account information.[143] And in 2016, Microsoft filed a lawsuit challenging the gag order provision of the 1986 Electronic Communications Privacy Act on both Fourth Amendment and First Amendment grounds.[144] A federal judge found in February 2017 that Microsoft had standing under the First Amendment to move forward with its challenge.[145]

C. Why Corporations Are Better Situated for Getting into Court

The current structure of U.S. surveillance law largely leaves citizens disempowered. Often, surveillance is secret, citizens do not even know they are being surveilled, and thus have no way to challenge the surveillance. I wholeheartedly agree with critics of this system, and believe that the current level of secrecy is deeply problematic.[146] Corporations are far from perfect stand-ins for citizen rights.[147]

However, in our imperfect world, the ethical corporation should stand up on behalf of its consumers. Companies know far more about the extent of government surveillance than users do.[148]

Bringing this Article's discussion of standing full circle: Companies are also better situated to assert surveillance challenges than individ-

141. Twitter, Inc. v. Holder, 183 F. Supp. 3d 1007, 1010 (N.D. Cal. 2016).

142. Elizabeth Banker, #*Transparency Update: Twitter Discloses National Security Letters*, TWITTER BLOG (Jan. 27, 2017), https://blog.twitter.com/2017/transparency-update-twitter-discloses-national-security-letters.

143. Dan Levine, *Judge Rules that Justice Dept. Can't Indefinitely Gag Yahoo on Subscriber Info Subpoena* (Feb. 6, 2015, 8:40 PM), http://www.rawstory.com/2015/02/judge-rules-that-justice-dept-cant-indefinitely-gag-yahoo-on-subscriber-info-subpoena/.

144. Steve Lohr, *Microsoft Sues Justice Department to Protest Electronic Gag Order Statute*, N.Y. TIMES (Apr. 14, 2016), http://www.nytimes.com/2016/04/15/technology/microsoft-sues-us-over-orders-barring-it-from-revealing-surveillance.html.

145. *See* Microsoft Corp. v. U.S. Dep't of Justice, No. C16-0538JLR, 2017 WL 530353, at *6 (W.D. Wash. Feb. 8, 2017). The court did not evaluate third-party standing under the First Amendment because it found that Microsoft had standing to sue on its own behalf. *Id.* at *14 ("Microsoft therefore need not show third-party standing as to its First Amendment claim.").

146. Cover, *supra* note 134, at 1501 ("[I]ndividuals should normally receive notice of government surveillance and acquisition of their data.").

147. *Id.* at 1441.

148. Rozenshtein, *supra* note 122, at 44 ("Because surveillance intermediaries are intimately familiar with the details of the surveillance programs with which they are required to cooperate, they avoid the knowledge problems that doom other plaintiffs.").

ual users. *Amnesty*'s requirement that a plaintiff show "certainly impending" harm presents a significant challenge for a person who has been given no notice that she is subject to government surveillance. By contrast, a company that knows who has definitely been surveilled is better situated to bring third-party challenges to the substance of surveillance orders. Companies can also enable users to know whether they have in fact been surveilled. Microsoft, for example, has standing to challenge the gag order provisions in the Electronic Communications Privacy Act because it can definitively point to a check on its ability to speak.[149] If the gag orders are lifted, then individuals will be better situated to show injury in fact for purposes of their own claims.

At least some companies can assert standing on behalf of their users. Wikimedia asserted third-party standing on behalf of its users in a recent challenge to national security Upstream surveillance.[150] Courts have held in the First Amendment context that entities, such as newspapers and internet service providers, have standing to assert the rights of their readers and posters.[151] In the recent Microsoft ECPA litigation, however, the district court rejected the assertion of third-party standing for Fourth Amendment claims.[152] The court was silent as to whether Microsoft could assert third-party First Amendment claims.[153] In 2008, however, the FISA court of appeals held that Yahoo could assert third-party standing for Fourth Amendment claims on behalf of its users.[154]

Companies and non-profit organizations can potentially use their sheer size, compared to individual users, to assert a likelihood of

149. *Microsoft Corp*., 2017 WL 530353, at *6.

150. Brief for Plaintiffs-Appellants at 61, Wikimedia Found. v. Nat'l Sec. Agency, No. 15-2650 (4th Cir. Feb 17, 2016), 2016 WL 703452, at *61. Again, full disclosure: I participated as author of an amicus brief. *See* Brief of Amici Curiae First Amendment Legal Scholars in Support of Plaintiffs-Appellants and Supporting Reversal at 1, *Wikimedia*, No. 15-2650 (4th Cir. Feb. 24, 2016), https://www.aclu.org/legal-document/wikimedia-v-nsa-amicus-brief-first-amendment-legal-scholars.

151. *See, e.g.*, McVicker v. King, 266 F.R.D. 92, 95–96 (W.D. Pa. 2010); Enterline v. Pocono Med. Ctr., 751 F. Supp. 2d 782, 786 (M.D. Pa. 2008).

152. *Microsoft Corp*., 2017 WL 530353, at *16 ("[T]he Supreme Court and the Ninth Circuit have routinely held in a variety of circumstances that a plaintiff may not assert the Fourth Amendment rights of another person.").

153. *Microsoft Corp*., 2017 WL 530353, at *14 ("Microsoft therefore need not show third-party standing as to its First Amendment claim.").

154. *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1008–09 (FISA Ct. Rev. 2008); *see* Rozenshtein, *supra* note 122, at 24 ("the Yahoo case relied on specific language in the FISA Statute, [but] it could become an important general precedent in surveillance cases if courts take a broad reading of its permissive approach to vindicating third-party rights.").

standing. Wikimedia pointed to the sheer number of its communications to argue a high probability that "the government is copying and reviewing at least some of its trillion or more annual communications."[155] The lower court rejected this claim; it remains to be seen as of publication of this Article whether the Fourth Circuit will be more amenable to it. If so, then companies will be able to more successfully assert "certainly impending" injury, since they are composed of many people, at least some of whom are likely to have been surveilled.

V. Conclusion

This Article has assessed the problem of privacy harms and Article III standing from a perhaps unconventional perspective. While privacy harms continue to trouble courts in the context of data breach and private data privacy litigation, in the national security surveillance context interesting and informative trends have emerged. In the national security context, courts appear to be prepared to recognize as harmful the interception of content, database storage and analysis, and a wider array of data-related harms. This Article argues that the chilling effect can be a recognized privacy harm, even in light of discouraging dicta in Supreme Court case law. Finally, this Article closed by returning to a theme of the *22nd Annual Clifford Symposium*: corporate responsibility. Companies are themselves driving changes in privacy law by challenging government surveillance and restrictions on their abilities to communicate with the public about surveillance. While relying on corporations to vindicate citizens' rights is problematic, recent lawsuits suggest that privacy—at least vis-a-vis the government—is in the wake of the Snowden leaks becoming a component of corporate responsibility.

155. Brief for Plaintiffs-Appellants, *supra* note 150, at 24.