Berkeley Technology Law Journal

Volume 29
Issue 4 *Annual Review 2014*

Article 20

8-1-2014

Standing in the Way of Privacy Protections: The Argument for a Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action

Lexi Rubow

Link to publisher version (DOI)
https://doi.org/10.15779/Z38T395

STANDING IN THE WAY OF PRIVACY PROTECTIONS: THE ARGUMENT FOR A RELAXED ARTICLE III STANDING REQUIREMENT FOR CONSTITUTIONAL AND STATUTORY CAUSES OF ACTION

Lexi Rubow[†]

"That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection."[1]
– Samuel Warren & Louis Brandeis

The evolution of technology over the past few decades has had a profound impact on society. This change has been beneficial in countless ways, from the convenience of new communication technologies to the efficiency gains associated with electronic storage of employee and medical records. There are, however, personal and societal costs to new information technology. As more of individuals' lives take place online, where personal information can be digitally captured and stored, individuals "are placed in the uncomfortable position of not knowing who might have access to [their] personal and business e-mails, [their] medical and financial records, or [their] cordless and cellular telephone conversations."[2] Perhaps more troublingly, even where the law has evolved to protect individuals' privacy, current standing jurisprudence may place them in the "uncomfortable position of not knowing"[3] whether they will have access to the courts to enforce these rights. Consider the following scenarios:

---

† J.D. Candidate, 2015, University of California, Berkeley, School of Law.

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
2. Bartnicki v. Vopper, 532 U.S. 514, 541 (2001) (Rehnquist, C.J., dissenting).
3. *Id.*

Example A: In December 2009, a hacker infiltrated the database of a payroll-processing firm.[4] To compound the problem, the payroll-processing firm had retained its customers' employees' "personal and financial information for years after" their employment ended.[5] As a result, the hacker gained access to the "names, addresses, Social Security numbers, dates of birth, and bank account information" of 27,000 employees.[6]

Example B: Google told Safari Internet browser users that it would not track their Internet usage, as long as users retained Safari's default "do not track" browser setting.[7] In violation of this promise, Google circumvented Safari's cookie blocker and placed cookies on Safari users' computers, then used the cookies to track users' Internet activities for several months.[8] Google removed the cookies only after a Stanford researcher caught them in the act.[9]

Example C: In 2008, Congress amended the Foreign Intelligence Surveillance Act (FISA) to authorize surveillance of U.S. citizens' communications with non-U.S. persons outside of the United States.[10] A number of individuals, including attorneys and human rights workers, who engaged in sensitive international communications had to take expensive measures to protect their legitimate conversations with clients from government surveillance.[11] For example, many had to travel to the home countries of their international clients in order to converse in confidence.

Aside from invoking similar privacy concerns, these stories share one key trait: the plaintiffs in each case failed to persuade their respective court to even address their substantive claims. Instead, before even *considering the merits* of the plaintiffs' claims, each court held that the plaintiffs had not suffered an injury-in-fact, and therefore lacked standing to sue.[12]

---

4. Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (2012).

5. Reilly v. Ceridien Corp., No. 10-5142, 2011 WL 735512, at *1 (D.N.J. Feb. 22, 2011).

6. *Reilly*, 664 F.3d at 40.

7. *See In re* Google, Inc. Cookie Placement Consumer Privacy Litigation, MDL Civ. No. 12-2358, 2013 WL 5582866, at *2–4 (D. Del. Oct. 9, 2013).

8. *Id.*

9. Kelly Fiveash, *FTC Urged to Probe Google's Safari-Tracking Gaffe*, THE REGISTER (Feb. 20, 2012), http://www.theregister.co.uk/2012/02/20/google_bypasses_apple_safari_privacy/.

10. *See* Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1144 (2013) (describing FISA as permitting surveillance of people reasonably believed to be located outside of the United States, which could include communications surveillance targets have with U.S. nationals).

11. *Id.* at 1145–46.

12. Reilly v. Ceridien Corp., No. 10-5142, 2011 WL 735512, at *7 (D.N.J. Feb. 22, 2011); *In re Google*, at 7; *Clapper*, 133 S. Ct. at 1154–55.

Privacy law plaintiffs have encountered great difficulty in establishing standing because the abstract and context-specific nature of privacy harm does not fit well with current, rigid judicial conceptualizations of injury-in-fact. In attempting to define injury-in-fact in the privacy setting, some courts attempt to analogize to older doctrine from other areas of law,[13] while others premise their findings of injury-in-fact on the probability that a particular event will occur.[14] These avenues of legal reasoning mask the fact that when judges determine whether a privacy plaintiff has suffered an "injury-in-fact," they are actually choosing one of many potential conceptualizations of privacy harm. This results in a decision-making process that is opaque at best and, at worst, denies court access to some plaintiffs that society may view as worthy of protection.

The Ninth Circuit recently introduced an alternative injury-in-fact standard, finding standing upon the plaintiffs' showing of a statutory violation.[15] This Note contrasts the Ninth Circuit's approach with the Supreme Court's recent government surveillance decision in *Clapper v. Amnesty International,* which followed the more conventional practice of divorcing the substantive cause of action analysis from the procedural injury-in-fact analysis.[16] Although different issues are at play in statutory versus constitutional causes of action, this Note explains that the Ninth Circuit's approach best fits the policies underlying standing doctrine for both types of claims.

Part I explores the problem of applying the injury-in-fact requirement to privacy issues and describes two alternative formulations of privacy harm. Parts II and III summarize the current state of standing jurisprudence in the constitutional and private-sector statutory context, respectively, and demonstrate that in each instance courts choose among a variety of conceptualizations of privacy. Part IV analyzes the Supreme Court's recent *Clapper* decision and the Ninth Circuit's approach in light of the various goals underlying standing doctrine. Finally, Part V concludes that, especially in the privacy context, the Ninth Circuit's approach offers the preferable method for analyzing injury-in-fact.

13. *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 638–39 (7th Cir. 2007) (analogizing data breaches to tort liability for exposure to harmful substances).

14. *See, e.g.*, *Clapper*, 133 S. Ct. at 1150 (dismissing plaintiffs' concerns as a "speculative chain of possibilities" insufficient to grant standing).

15. Edwards v. First Am. Corp., 610 F.3d 514, 517 (9th Cir. 2010).

16. *See Clapper*, 133 S. Ct. at 1147.

I. INJURY-IN-FACT VS. PRIVACY HARM

This Part begins by explaining the injury-in-fact requirement and the difficulty of applying such a requirement to privacy harms. It then describes two example conceptualizations of privacy harm. It concludes by introducing an alternative method of analyzing injury-in-fact that better comports with the varied and contextual nature of privacy harms.

A. THE DISCONNECT BETWEEN ARTICLE III STANDING AND PRIVACY HARMS

Standing is "a question of access apart from the merits of the controversy,"[17] addressing "whether a specific person is the proper party to bring a matter to the court."[18] Standing requirements derive from the "case or controversy" clause in Article III of the Constitution.[19] Although the clause does not explicitly mention standing, in the late twentieth century, the Supreme Court began using this clause to limit the types of plaintiffs and cases that it would entertain.[20] Over the next few decades, the Court elaborated on the elements required to establish a "case or controversy" under Article III. Current precedent requires plaintiffs to establish that they suffered an injury that is (1) "concrete, particularized," and "actual or

17. Steven L. Winter, *The Metaphor of Standing and the Problem of Self-Governance*, 40 STAN. L. REV. 1371, 1255 (1988).

18. ERWIN CHEMERINSKY, FEDERAL JURISDICTION 56 (4th ed. 2003).

19. The "case or controversy" clause of Article III reads as follows:

> The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority;--to all Cases affecting Ambassadors, other public ministers and Consuls;--to all Cases of admiralty and maritime Jurisdiction;--to Controversies to which the United States shall be a Party;--to Controversies between two or more States;--between a State and Citizens of another State;--between Citizens of different States;--between Citizens of the same State claiming Lands under Grants of different States, and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.

U.S. CONST. art. III, § 2, cl. 1. Notably, the clause does not mention most of the modern "Article III standing" requirements, including injury-in-fact. *See id.*

20. Scholars have described the development of the doctrine as a response to the rapid expansion of federal dominance corresponding with the rise of the modern administrative state. *See* Winter, *supra* note 17, at 1455. Standing was a tool used to exercise "expansive federal judicial power in the economic sphere to invalidate progressive legislation." *Id.* The development of standing doctrine also corresponded with the rise of liberalism, which "focuses upon a regime that achieves agreement on process rather than end goals." *Id.* at 1454.

imminent"; (2) "fairly . . . trace[able] to the challenged action"; and (3) "redress[able] by a favorable decision."[21]

The first prong, known as the injury-in-fact requirement, does not pose much of a burden for harms that the law has traditionally recognized. Physical injuries were one of the first types of harm that the law sought to prevent,[22] and, as such, few would dispute that the victim of a battery, for example, has suffered a legally cognizable harm.[23] Similarly, causes of action for economic harms, such as trespass to chattels or breach of contract, have existed since the English common law.[24] When confronting these traditional types of harm, courts rarely even address the issue of standing. Instead, the question of whether a plaintiff has met the injury-in-fact requirement typically arises in cases where the plaintiff asserts a harm for a newly evolving legal protection.[25]

Loss of privacy is one such harm. Samuel Warren and Louis Brandeis first contemplated legal protection for privacy at the end of the nineteenth century in their influential article *The Right to Privacy*.[26] Writing in response to new developments in photographic technology that allowed users to instantaneously take pictures, Warren and Brandeis noted that "modern enterprise and invention have, through invasions upon his privacy, subjected [the modern individual] to mental pain and distress, far greater than could be inflicted by mere bodily injury."[27] Thus, they concluded, the law should evolve to protect individuals' "right to be let alone."[28]

---

21. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992). Courts also subject cases to a second round of discretionary or "prudential" standing requirements. CHEMERINSKY, *supra* note 18 at 60. These requirements are outside the scope of this Note.

22. *See* Warren & Brandeis, *supra* note 1, at 193 ("[I]n very early times, the law gave a remedy only for physical interference with life and property.").

23. In fact, "harm" is incorporated in the definition of battery. The Restatement (Second) of Torts, lists "a *harmful* contact with the person of the other" as one of the elements of battery. RESTATEMENT (SECOND) OF TORTS § 13 (1965) (emphasis added). This would be a tautology were it not so well-established that physical injury is, in fact, a "harm."

24. *See generally* W.T. BARBOUR, THE HISTORY OF CONTRACT IN EARLY ENGLISH EQUITY (1914), *available at* http://socserv2.socsci.mcmaster.ca/econ/ugcm/3ll3/barbour/HistoryContract.pdf.

25. *See, e.g.*, Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992) (environmental groups asserting interest in environmental protection of federal land); Sierra Club v. Morton, 405 U.S. 727 (1972) (conservationist group asserting "a special interest in the conservation and the sound maintenance of the national parks"); United States v. Students Challenging Regulatory Agency Procedures (SCRAP), 412 U.S. 669 (1973) (environmental groups challenging increase in federal freight rates).

26. *See* Warren & Brandeis, *supra* note 1.

27. *Id.* at 196.

28. *Id.* at 193.

Since that time, various government entities have noted the privacy implications of evolving technologies and have created a number of causes of action to protect consumers from invasions of their privacy.[29] However, courts have struggled to apply the injury-in-fact requirement to cases arising under these new causes of action. At least some of this difficulty stems from the wide variety of conceptualizations of privacy harm, some or all of which may be appropriate in any given context.

B. ALTERNATIVE FORMULATIONS OF PRIVACY HARM: CONTROL AND INTELLECTUAL PRIVACY THEORIES

This section attempts to demonstrate the varied and context-specific nature of privacy harm by exploring two sample conceptualizations of privacy harm: "control theory"[30] and "intellectual privacy theory."[31]

Control theorists conceptualize privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[32] It "is not simply an absence of information about what is in the minds of others; rather it is the control we have over information about ourselves."[33] Loss of this control results in "a suffocating powerlessness and vulnerability."[34] The psychological toll of such helplessness is exemplified by Franz Kafka's *The Trial*, where the protagonist unsuccessfully attempts to navigate a cryptic and impenetrable legal bureaucracy.[35] The bureaucratic aggregation of individuals' personal information, and associated "indifference, errors, abuses, frustration and lack of transparency and accountability," inflicts harm by excluding "the protagonist from having any knowledge or participation in the process."[36]

Intellectual privacy theory constitutes an alternative formulation of privacy. This theory describes privacy as necessary for the "conscious

---

29. *See*, *e.g.*, Health Insurance Privacy and Portability Act ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (2002) (regulating health information); Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710 (2012) (protecting privacy of video rental records); Cal. Civ. Code §§ 1798.29, 1798.82, 1798.84 (protecting general security of personally identifying information); Internet Security and Privacy Act, N.Y. State Tech. Law § 208 (same).

30. *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

31. *See, e.g.*, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000).

32. WESTIN, *supra* note 30, at 7.

33. Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968).

34. Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 766 (2007).

35. FRANZ KAFKA, THE TRIAL (1925).

36. Solove, *supra* note 34, at 766.

construction of self" and development of autonomous thought.[37] Some intellectual privacy scholars analogize sustained loss of privacy to Jeremy Bentham's "panopticon"—a circular prison building with cells facing the center, such that a guard standing in the center can view any cell at any time.[38] The panopticon's prisoners, aware that the guard may be watching, begin to censor or discipline themselves.[39] Similarly, individuals experiencing sustained or repeated loss of privacy begin to constrain themselves in order to preempt societal rebuke.[40] Professor Julie Cohen writes:

> The point is not that people will not learn under conditions of no-privacy, but that they will learn differently, and that the experience of being watched will constrain, ex ante, the acceptable spectrum of belief and behavior. Pervasive monitoring of every first move or false start will at the margin, incline choices toward the bland and the mainstream. The condition of no-privacy threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it . . . .[41]

Preventing individuals from developing channels of independent thought inhibits "society's foundational commitments to intellectual diversity and eccentric individuality."[42]

The types of harm implicated by any given privacy law issue will likely vary by context. As Professor Daniel Solove argues, trying to fit any given privacy problem "into a one-size-fits-all conception of privacy neglects to see the problem[] in [its] full dimensions or to understand [it] completely."[43] Privacy law covers a wide range of actions that impinge on personal privacy, including surveillance, interrogation, information processing, information dissemination, or unauthorized access to information.[44] Control theory, intellectual privacy theory, or other formulations of harm may be of varying relevance, depending on the type of privacy violation in question. Thus, Solove argues that "[w]e should conceptualize privacy by focusing on the specific types of disruption and the specific practices disrupted rather than looking for the common denominator that links all of them."[45]

---

37. Cohen, *supra* note 31, at 1424.

38. Bert-Jaap Koops, *Law, Technology, and Shifting Power Relations*, 25 BERKELEY TECH. L.J. 973, 993 (2010).

39. *Id.* at 995.

40. *See* Cohen, *supra* note 31, at 1426.

41. *Id.*

42. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1948 (2013).

43. Solove, *supra* note 34, at 759.

44. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 488–91 (2006).

45. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1130 (2002).

This contextually sensitive approach to defining privacy-related harms is at odds with standing jurisprudence, which requires judges to apply a baseline standard of harm without any reference to the underlying cause of action. As a result, many courts "simply analyze the issues without articulating a conception of what privacy means. However, conceptualizing privacy is essential for the analysis of these issues."[46]

C. JUDGE FLETCHER AND THE NINTH CIRCUIT'S APPROACH TO STANDING

In his article *The Structure of Standing*, Judge William Fletcher of the Ninth Circuit introduces a new way of analyzing standing that may be better suited to address privacy harms.[47] Judge Fletcher argues that courts should "abandon the attempt to capture the question of who should be able to enforce legal rights in a single formula."[48] Instead, whether or not a plaintiff has sustained an injury "must be seen as part of the question of the nature and scope of the substantive legal right on which plaintiff relies."[49] Ultimately, Judge Fletcher concludes that causes of action carry with them implicit definitions of harm, and courts should not attempt to override this definition of harm with their own.[50] Access to the courts should be coextensive with possessing a meritorious claim pursuant to the underlying cause of action.[51]

Judge Fletcher's approach is particularly attractive in the relatively nascent and abstract field of privacy law. As discussed above, the type of harm underlying a privacy cause of action may not fit well with traditional ideas of injury-in-fact. Judge Fletcher's approach allows the entity defining the scope of the underlying cause of action to determine, implicitly or explicitly, the types of harm that are worthy of protection.

In *Edwards v. First American*,[52] a Ninth Circuit panel, including Judge Fletcher, adopted a limited form of Judge Fletcher's standing approach, finding standing based on the defendant's statutory violation and thereby essentially merging the injury-in-fact standing question with the underlying cause of action.[53] Courts in the Ninth Circuit have since applied this standing approach to a string of privacy cases, granting plaintiffs standing if they

46. Solove, *supra* note 34, at 754.
47. William A. Fletcher, *The Structure of Standing*, 98 YALE L. J. 221 (1988).
48. *Id.* at 223.
49. *Id.* at 232–33.
50. *Id.*
51. *Id.*
52. 610 F.3d 514 (9th Cir. 2010).
53. *See id.* at 517–18.

establish a *per se* violation of a privacy statute, regardless of whether they suffered economic harm.[54]

The following two Parts summarize the majority approach in the government surveillance and statutory privacy law contexts, as well as the Ninth Circuit's approach to statutory standing. These Parts demonstrate that the type of injury-in-fact required by current precedent only addresses one out of many possible conceptualizations of harm. The remainder of the Note will then analyze the implications of the majority and Ninth Circuit approaches.

II. DEFINING INJURY-IN-FACT FOR CLAIMS ARISING UNDER CONSTITUTIONAL CAUSES OF ACTION

The Supreme Court's decision in *Clapper v. Amnesty International* exemplifies the judicial practice of analyzing injury-in-fact divorced from the harms implicated by the underlying cause of action. Although the Court's decision appears to be based on a purely factual assessment of probability, this Part demonstrates that the Court still chose one of many definitions of harm.

A. CLAPPER V. AMNESTY INTERNATIONAL: THE MAJORITY OPINION

In *Clapper*, plaintiffs challenged the constitutionality of the 2008 Amendments to FISA, which expanded the government's authority to conduct surveillance.[55] Among other things, under the Amendments the government need not show that international targets are agents of a foreign power, only that they are not "United States persons."[56]

In response to the FISA amendments, a group of U.S. lawyers, human rights workers, and other persons whose work involved "sensitive international communications with individuals who they believe[d were] likely targets of surveillance"[57] brought a class action lawsuit against the government challenging the amendments' constitutionality pursuant to the "Fourth Amendment, the First Amendment, Article III, and separation of powers principles."[58] The plaintiffs offered two theories for demonstrating the injury-in-fact element of Article III standing: (1) the "objectively

54. *See, e.g.*, *In re* Hulu Privacy Litigation, No. C 11-03764 LB, 2012 WL 2119193 (N.D. Cal. June 11, 2012); *In re* Facebook Privacy Litigation, 791 F. Supp. 2d 705 (N.D. Cal. 2011).

55. Amnesty Int'l v. Clapper, 133 S. Ct. 1138, 1142–44 (2013).

56. *Id.*

57. *Id.* at 1142.

58. *Id.* at 1146.

reasonable likelihood" that they would suffer future injury due to acquisition of their communications,[59] and (2) present injury due to "costly and burdensome measures [taken] to protect the confidentiality of their international communications."[60] The plaintiffs asserted that the FISA amendments "compromise[d] their ability to locate witnesses, cultivate sources, obtain information, and communicate confidential information to their clients," such that they had to travel abroad to speak with clients in person rather than "engag[e] in certain telephone and e-mail conversations."[61]

The Southern District of New York rejected these arguments, but the Second Circuit reversed, holding that as long as there was an "objectively reasonable likelihood" that the plaintiffs would be the targets of surveillance, plaintiffs had standing to sue.[62] In particular, the court held that the plaintiffs' "fears of surveillance" were "based on a reasonable interpretation of the challenged statute and a realistic understanding of the world."[63] The Second Circuit further held that the plaintiffs' precautionary measures caused harm sufficient to establish Article III standing, since they were taken in response to a fear of government action that was not "fanciful, paranoid, or otherwise unreasonable."[64]

The Supreme Court, in a 5-4 decision, rejected the Second Circuit's "objectively reasonable likelihood" standard.[65] Instead, the Supreme Court held that in order to establish injury-in-fact based on a potential future injury, that injury must be certainly impending.[66] The Court held that the plaintiffs' argument failed to meet this standard, as the likelihood that the government would actually target their conversations rested on "a highly attenuated chain of possibilities."[67] First, the Government would have to decide to target the communications of the plaintiffs' foreign contacts.[68] Second, the Foreign Intelligence Surveillance Court (FISC), the judicial body charged with approving ex parte surveillance applications, would need to "conclude that the Government's proposed surveillance procedures satisfy [FISA's] many

59. *Id.*
60. *Id.* at 1143.
61. *Id.* at 1145–46 (internal quotations omitted).
62. *Id.* at 1146.
63. Amnesty Int'l v. Clapper, 638 F.3d 118, 139 (2d Cir. 2011).
64. *Id.* at 134.
65. *Clapper*, 133 S. Ct. at 1154.
66. *Id.* at 1147–48.
67. *Id.* at 1148.
68. *Id.*

safeguards and are consistent with the Fourth Amendment."[69] Third, the Government would need to succeed in intercepting the specific communications in which the plaintiffs participated.[70]

The plaintiffs' present injury arguments did not fare much better. The Court held that to establish standing based on precautionary measures taken in response to fear of government action, the plaintiffs still must demonstrate that the feared government action is certainly impending.[71] The Court explained that plaintiffs "cannot manufacture standing" by undertaking protective measures.[72] Even if this fear had the effect of chilling the plaintiffs' protected speech, the Court held 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."[73]

B. ALTERNATIVE DEFINITIONS OF HARM

All discussions of probability aside, the Court's equating "harm" with actual interception of the plaintiffs' conversations was, itself, a choice from among many potential definitions of harm. Although the Court did not explain its choice of definitions, control theory may, in part, justify the Court's decision, as actual interception would indicate that the plaintiffs actually lost control of their data.

However, control theory goes beyond this understanding of harm. In fact, Solove argues that from a control theory perspective, "[t]he NSA programs are problematic even if no information people want to hide is uncovered."[74] Comparing the NSA surveillance program to Kafka's *The Trial*, Solove argues that NSA surveillance problematically evokes "a suffocating

---

69. *Id.*

70. *Id.* The Court further found that the plaintiffs' arguments failed to establish that any alleged harm would be "fairly traceable" to the FISA amendments, since even if the plaintiffs were targeted, the Government could invoke its authority under a variety of surveillance methods. *Id.* at 1149.

71. *Id.* at 1151.

72. *Id.*

73. *Id.* at 1152. Quoting its 1972 case *Laird v. Tatum*, the Court explained that:

> While acknowledging that prior cases had held that constitutional violations may arise from the chilling effect of 'regulations that fall short of a direct prohibition against the exercise of First Amendment rights,' the Court declared that none of those cases involved a 'chilling effect aris[ing] merely from the individuals' knowledge that a governmental agency was engaged in certain activities.

Id. at 1152 (quoting Laird v. Tatum, 408 U.S. 1, 13–14 (1972).

74. Solove, *supra* note 34, at 766.

powerlessness and vulnerability."[75] The secrecy of NSA programs prevents people "from having knowledge about how their information is being used, [and bars them] from being able to access and correct errors in that data."[76] Regardless of whether the government actually intercepted the plaintiffs' communications, the question of whether the government attempts such an interception lies completely out of the plaintiffs' control—it is the government's choice alone. Thus, even though the Supreme Court found that the plaintiffs failed to meet the Court's "certainly impending" standard,[77] the plaintiffs may still have suffered harm stemming from the loss of control of their own personal information.

Similarly, under the intellectual privacy theory of harm, it would not matter whether the government actually intercepted plaintiffs' conversations. As in Bentham's panopticon, the government need not actually watch any given U.S. citizen; the belief that the government could be watching at any time potentially causes U.S. citizens—like the plaintiffs—to preemptively censor themselves out of fear of such invasive surveillance.[78]

Both the pure control theory and the intellectual privacy theory do present justiciability problems. Because the harms described under both theories stem from the individual's subjective perception of privacy loss, applying either theory in its purest form would mean granting access to individuals, even if their perceptions are irrational or paranoid. The Second Circuit's "objectively reasonable likelihood" standard adeptly achieved the goal of protecting intellectual privacy harms on the societal level, while weeding out irrational or paranoid claims.[79] Knowledge of widespread surveillance under FISA certainly supports a reasonable fear that U.S. citizens will be targets of surveillance when communicating with clients in volatile areas of the world.[80] Further, the Clapper plaintiffs offered concrete evidence of self-censorship, explaining that they refrained from saying certain things to clients over the phone and travelled abroad in order to speak more freely.[81]

This analysis demonstrates that the Court's holding was not purely a factual determination of probability. Instead, the Court's equating "harm" to actual interception of the plaintiff's conversation reflected a choice. Whether or not the Court selected the "correct" definition of harm for this context,

75. *Id.*
76. *Id.* at 766–67.
77. *See Clapper*, 133 S. Ct. at 1154.
78. *See* Koops, *supra* note 38, at 993.
79. *See* Amnesty Int'l v. Clapper, 638 F.3d 118, 135–36 (2d Cir. 2011).
80. *Amnesty Int'l*, 638 F.3d at 134.
81. *Clapper*, 133 S. Ct. at 1164 (Breyer, J., dissenting). *Cf.* Solove, *supra* note 34, at 766 ("[I]t is often very hard to demonstrate concrete evidence of deterred behavior.").

the fact that it offered no explanation as to why it selected this definition of harm over any of the many rivaling definitions—and particularly the fact that it did so with little consideration of the harms that the Fourth or First Amendments might represent—is troubling.

III. DEFINING INJURY-IN-FACT FOR CLAIMS ARISING UNDER STATUTORY CAUSES OF ACTION

The same difficulties of defining injury-in-fact also bedevil privacy claims arising under statutory causes of action. The majority of jurisdictions also require plaintiffs alleging *statutory* privacy violations to meet a judicially determined standard of injury-in-fact separate from the underlying cause of action. Despite the fact that a number of these statutes provide a private right of action,[82] plaintiffs struggle to allege facts sufficient to meet the required separate, judicially-defined conception of injury-in-fact.

A. THE MAJORITY RULE: JUDICIALLY ASSIGNED HARM DEFINITION

Courts assessing standing for private-sector privacy cases have used a number of standards of injury-in-fact. Some courts attempt to analogize privacy causes of action to other, more established areas of tort law.[83] Others take a similar approach to the *Clapper* Court, equating the occurrence of a particular event to "harm," then premising standing on the likelihood of that event occurring in the future.[84] Although a full canvas of standing jurisprudence in each area of sectoral privacy law lies beyond the scope of this Note, the following examples demonstrate that courts following the majority practice of defining injury make an active choice by selecting one definition of harm from many.

In *Pisciotta v. Old National Bancorp*, the Seventh Circuit analogized the harm stemming from a data breach[85] to the "increased risk" theory of harm

82. *See, e.g.*, Wiretap Act, 18 U.S.C. §§ 2511(5), 2520 (2012); Stored Communications Act, 18 U.S.C. § 2712 (2012); Fair and Accurate Credit Transactions Act, 15 U.S.C. §§ 1681 et seq. (2012).

83. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (analogizing data breaches to toxic tort liability).

84. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (rejecting plaintiffs' claims because they failed to show a "certainly impending" injury or one with a "high degree of immediacy").

85. "A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so." *Definition: Data Breach*, TECHTARGET (May 2010), http://searchsecurity.techtarget.com/definition/data-breach.

that some courts utilize in the toxic tort context.[86] In *Pisciotta*, a hacker improperly accessed the computer system of a financial services provider, exposing the plaintiffs' personal information but resulting in no realized financial loss or identity theft.[87] In analyzing whether there had been an injury-in-fact, the court analogized the case at hand to environmental exposure tort cases, which granted plaintiffs standing upon demonstration that the act "increase[d] the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions."[88] The court granted standing on this basis.

On a similar set of facts, the Third Circuit in *Reilly v. Ceridian Corp*. used a "likelihood of future harm" approach to determine whether there had been an injury-in-fact.[89] In *Reilly*, a hacker accessed the database of a payroll and human resources management company, exposing clients' employees' "names, addresses, social security numbers, dates of birth, and bank account information."[90] The *Reilly* court's analysis mirrored the analysis in *Clapper* and arrived at the same result: although plaintiffs had "incurred costs to monitor their credit activity,"[91] the likelihood that their information would be abused was too attenuated for plaintiffs to establish standing to sue.[92] The court reasoned that plaintiffs would need to demonstrate that a malicious third party "(1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names."[93] The court held that "[u]nless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm."[94]

Although the *Pisciotta* and *Reilly* courts analyzed harm in different ways, the two cases represent the majority trend of requiring plaintiffs to meet a

86. *See* Miles L. Galbraith, Note, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U. L. REV. 1365, 1388–96 (2013).

87. *Pisciotta*, 499 F.3d at 631–32.

88. *Id.* at 634.

89. *Reilly*, 664 F.3d at 42.

90. *Id.* at 40.

91. *Id.*

92. *Id.*; *see* Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1148-49 (2013).

93. *Reilly*, 664 F.3d at 42.

94. *Id.*; *see also* Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (holding no injury-in-fact where an electronic brokerage management system used insufficient encryption methods, thereby exposing plaintiffs' information, absent any evidence that the plaintiffs' data was "accessed by one or more unauthorized parties").

judicially determined standard of injury-in-fact separate from the underlying cause of action. And, as in *Clapper*, the courts' reasoning for defining harm in a particular way is all but clear. The court in *Pisciotta* found standing without addressing the harms underlying the privacy cause of action, finding injury-in-fact by way of analogy to tort law.[95] The court in *Reilly* interpreted injury-in-fact to mean actual abuse of the plaintiffs' data.[96] Although both of these definitions appear to follow logically from the most basic and easily cognizable harm—physically tangible harm—the courts could have selected any number of alternate definitions. As in *Clapper*, neither court explained its process or reasoning for selecting this definition of harm to the exclusion of alternate definitions.

For example, a control theory analysis would likely suggest that harm arises not only from misuse of the data but also from the breach itself. In both *Pisciotta* and *Reilly*, customers chose to share information with a trusted institution for a particular purpose; when malicious third parties hacked the defendants' computer systems, customers lost control over who had access to their personal information.[97] The probability need not be nearly as high as the *Reilly* court would require for the breach to cause feelings of powerlessness and anxiety.

The *Pisciotta* court's "increased risk" analysis overlaps with control theory, but it is not coextensive. Harm under control theory would not necessarily require an increased risk of exposure, as the harmful sense of powerlessness stems from the *perception* of loss of control over personal information, regardless of whether an increased risk of harm can be statistically proven. However, this sense of powerlessness is likely enhanced in a situation where data breach increases the risk of exposure, since increased risk likely corresponds to increased perception of loss of control.

These courts could have alternately applied the personhood theory, although the connection to personhood theory is more tangential. If individuals generally lose faith in electronic storage practices and become concerned that their data is unsafe in the hands of third parties as a result of the data breach, they may begin to avoid or censor their data-generating activities in order to preempt their exposure. Again, because such a response would stem from individuals' perceptions, this harm could occur regardless of the probability of future harm or whether breach has increased that probability.

95. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007).
96. *Reilly*, 664 F.3d at 42.
97. *See Pisciotta*, 499 F.3d at 632; *Reilly*, 664 F.3d at 40.

However, this line of analysis would lead to justiciability problems, because the loss of faith argument could also extend to those who have not even been victim to the data breach. For example, when online shopping technologies first entered the marketplace, many users feared that their transactions would not be secure and therefore refrained from making purchases online.[98] Thus, self-censorship or feelings of anxiety over control of information can arise from the fear of new technologies or from observation of others' compromised personal information. But, even if courts were to consider such an open-ended definition of harm, the underlying cause of action could curtail lawsuits from parties whose data was not actually breached.

Thus, while some definitions of harm are more applicable or feasible than others in the privacy breach context, the availability of multiple definitions of harm indicates that the courts in question did make a choice to select some types of harm over others for the purpose of evaluating standing, with little explanation. Regardless of whether one views the outcome of such decisions as correct, the reasoning behind selecting the chosen definition is incredibly opaque—perhaps even to the judges rendering the decisions—and therefore runs the risk of excluding plaintiffs who have suffered harm according to the underlying cause of action but not according to the harm the judge elects to evaluate for establishing injury-in-fact.

B. *EDWARDS* AND THE NINTH CIRCUIT RULE: STATUTORY VIOLATION AS STANDING

With its decision in *Edwards v. First American Financial Corp*,[99] the Ninth Circuit established a new way of addressing the injury-in-fact requirement of Article III standing: leaving the definition to the legislature's discretion. In *Edwards*, the Ninth Circuit held that statutes that grant plaintiffs a private right to enforce statutory violations also impliedly grant plaintiffs standing to do so.[100] In *Edwards*, the plaintiff alleged that referral agreements between title insurers and agencies violated the Real Estate Settlement Procedures

98. *See* Sabine Einwiller, *The Significance of Reputation and Brand for Creating Trust in the Different Stages of a Relationship between an Online Vendor and its Customers*, Proceedings of the Eighth Research Symposium on Emerging Electronic Markets, at 1–2 (September 2001), *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.58.2482&rep=rep1&type=pdf (discussing consumers' initial concerns with the "privacy, security of monetary transactions, legal regulations, and proper delivery" of online commercial transactions in the early stages of online commerce).

99. 610 F.3d 514 (9th Cir. 2010).

100. *Id.* at 517.

Act.[101] This Act did not premise recovery on plaintiffs' showing actual damages; the Act permitted plaintiffs to recover merely upon a showing that the defendant violated the statute.[102] The court reasoned that if the legislature intended to grant damages on the basis of a statutory violation alone, it also implicitly intended for the plaintiff to have standing to pursue such damages.[103] Thus, the court held that although the plaintiff did not "allege[] that the charge for title insurance was higher than it would have been" without the statutory violation, and therefore could not establish any actual damages, the violation alone sufficed to establish standing.[104]

The Supreme Court granted certiorari and heard arguments on *Edwards*. Although *Edwards* did not involve privacy law, a number of technology companies and consumer privacy advocates noted the impact that *Edwards* would have on statutory privacy law and filed amicus briefs.[105] The Court ultimately dismissed the writ as improvidently granted, allowing the Ninth Circuit to continue applying the *Edwards* standard and leaving in place a developing circuit split with broad implications for privacy law.[106]

As the amici predicted, the Ninth Circuit has since applied the *Edwards* standard to cases arising under privacy statutes. In *In re Hulu Privacy Litigation*,[107] the Ninth Circuit found that plaintiffs had established standing by alleging that Hulu had breached the Video Privacy Protection Act.[108] Specifically, Hulu customers "allege[d] that Hulu wrongfully disclosed their video viewing selections and personal identification information to third parties such as online ad networks."[109] Although the plaintiffs did not present any evidence that the third parties had misused their personal information, the Ninth Circuit held that the plaintiffs had established standing under *Edwards*.[110] They reiterated that "a plaintiff satisfies Article III's injury-in-fact

101. *Id.* at 515.
102. *Id.* at 517.
103. *Id.* at 518.
104. *Id.* at 516.
105. *See, e.g.*, Brief for Amici Curiae Facebook, Inc., LinkedIn Corp., Yahoo! Inc., and Zynga Inc. in Support of Petitioners, First Am. Fin. Corp. v. Edwards, 132 S. Ct. 2536 (2012) (No. 10-708), 2011 WL 3857211 (submitted by a coalition of technology companies); Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) in Support of the Respondent, First Am. Fin. Corp. v. Edwards, 132 S. Ct. 2536 (2012) (No. 10-708), 2011 WL 4957381 (submitted by an organization that advocates on privacy policy).
106. First Am. Fin. Corp. v. Edwards, 132 S. Ct. 2536 (2012).
107. No. C 11-03764 LB, 2012 WL 2119193 (N.D. Cal. June 11, 2012).
108. *Id.* at *8–*9.
109. *Id.* at *1.
110. *Id.* at *8.

requirement by alleging a violation of a statutorily-created legal right . . . [including] a consumer privacy statute with a private right of action."[111]

Similarly, in *In re Facebook Privacy Litigation*,[112] the Northern District of California held that plaintiffs had established standing by alleging that Facebook "transmitted personal information about Plaintiffs to third-party advertisers without Plaintiff's consent" in violation of the Wiretap Act.[113] Because the Wiretap Act provides for a private right of action,[114] the court held that the plaintiffs had established standing: "The injury required by Article III can exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'"[115]

The Ninth Circuit in *Edwards* thus established a method of defining injury-in-fact that is completely deferential to the type of harm that the legislature had in mind when creating the statute. Such a straightforward and consistent method of assessing standing differs from the more traditional, but more inscrutable, majority approach employed in cases like *Clapper, Reilly,* and *Pisciotta*. The underlying goals of modern standing doctrine provide insight into understanding the impact and possible rationale of each method, as well as their individual flaws.[116]

---

111. *Id.* at *7.

112. 791 F. Supp. 2d 705 (N.D. Cal. 2011).

113. *Id.* at 708.

114. *Id.* at 712 (quoting 18 U.S.C. § 2520(a) ("[A]ny person whose electronic communication is 'intercepted, disclosed, or intentionally used' in violation of the Act may in a civil action recover from the entity which engaged in that violation.").

115. *Id.* at 711 (quoting First Am. Fin. Corp. v. Edwards, 610 F.3d 514, 517 (9th Cir. 2010)) (internal quotation marks omitted); *see also* Graczyk v. West Pub. Co., 660 F.3d 275, 277 (7th Cir. 2011). In *Graczyk*, plaintiffs alleged that the DMV had sold the plaintiffs' records to West Publishing in violation of the Driver's Privacy Protection Act ("DPPA"), which prohibits unconsented disclosures of personal information. *Graczyk*, 660 F.3d at 276–77. The Seventh Circuit held that the plaintiffs had standing, as the DPPA gives private individuals a right of action: "The DPPA protects individuals from certain uses or disclosures of their personal information and creates a federal right of action for the same. . . . The plaintiffs allege . . . disclosure or use of the plaintiff's personal information that is prohibited by the DPPA. . . . The plaintiffs have therefore alleged an injury in fact." *Id.* at 278.

116. Strangely, in the Ninth Circuit it is much easier for plaintiffs to establish standing by framing the breach as a statutory violation than it would be if they had framed the same breach under a common law cause of action, because under a common law cause of action a plaintiff would need to independently establish injury-in-fact.. This poses another problem and is outside the scope of this Note.

IV. COMPARING CURRENT STANDING JURISPRUDENCE WITH THE GOALS UNDERLYING STANDING

Having established the current state of standing jurisprudence in the constitutional and statutory privacy law context, this Part now compares these different standards of injury-in-fact with the underlying policy goals of the standing doctrine. Dean Erwin Chemerinsky expertly outlines the goals of the Article III standing requirement as fourfold: (1) promoting the separation of powers, (2) increasing judicial efficiency, (3) improving judicial decision-making, and (4) ensuring fairness by requiring that parties are sufficiently invested in the outcome of the case.[117] This Part analyzes both traditional standing jurisprudence and the Ninth Circuit rule in light of these four goals and demonstrates that the policies underlying standing's injury-in-fact requirement do not support traditional standing jurisprudence in either the constitutional or statutory privacy law context.

A. PROMOTING THE BALANCE OF POWERS

One of the most prominent justifications for a stringent standing requirement argues that standing promotes the separation of powers by limiting the types of cases that the judicial branch can hear, thereby restricting its power in relation to the other two branches.[118] Justice Antonin Scalia wrote in strong support of this justification in his watershed journal article, *The Doctrine of Standing as an Essential Element of the Separation of Powers*.[119] Scalia noted that the Framers of the Constitution designed the judiciary to be removed from the whims of the majority so that it could serve the important role of "protecting individuals and minorities against impositions of the majority."[120] However, he argued, granting the judicial branch too much power creates problems. Not only does governance by an appointed body undermine the nation's democratic foundations, the judiciary is particularly ill-suited for dealing with all of the nation's issues:

> [Judges are] selected from the aristocracy of the highly educated, instructed to be governed by a body of knowledge that values abstract principle above concrete result, and . . . removed from all accountability to the electorate. That is just perfect for a body that is supposed to protect the individual against the people; it is just

117. CHEMERINSKY, *supra* note 18, at 57–59.

118. CHEMERINSKY, *supra* note 18, at 57 (advocating for "separation of powers by restricting the availability of judicial review").

119. Antonin Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 SUFFOLK U. L. REV. 881 (1983).

120. *Id.* at 894.

> terrible (unless you are a monarchist) for a group that is supposed to decide what is good for the people.[121]

Although this argument is persuasive when taken to the extreme, it does little to justify the current balance of powers. Current standing jurisprudence in the constitutional privacy law context, exemplified by *Clapper*, shifts the balance too far away from the judicial branch, such that U.S. citizens do not have any recourse to protect themselves against oppression by the legislative and executive branches. On the other hand, in the private-sector statutory privacy law context, the majority rule confers too much power on the judiciary, circumventing the legislature's attempts to protect consumers from evolving privacy threats and harms.

1. Constitutional Challenges

Traditional standing jurisprudence dictates an even higher degree of scrutiny "when reaching the merits of a dispute would force [the court] to decide whether an action taken by one of the other two branches of the federal government was unconstitutional."[122] However well-entrenched this axiom may be, current standing jurisprudence in the government surveillance context goes too far in the name of judicial restraint and, in doing so, frustrates the goals of the Framers of the Constitution.[123] For example, the Supreme Court's decision in *Clapper* effectively bars FISA surveillance from judicial review,[124] disrupting the balance of power in favor of the executive and legislative branches and tilting the scales of power in favor of the government at the expense of the governed.

---

121. *Id.* at 896.

122. Raines v. Byrd, 521 U.S. 811, 819–20 (1997). *See, e.g.*, Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1146 (2013) ("The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches.").

123. *See* THE FEDERALIST NO. 78, 469 (Alexander Hamilton) ("[W]here the will of the legislature, declared in its statutes, stands in opposition to that of the people, declared in the Constitution, the judges ought to be governed by the latter rather than the former.").

124. The Foreign Intelligence Surveillance Court ("FISC"), a special court composed of eleven federal district court judges, does hear surveillance warrant applications pursuant to the Foreign Intelligence Surveillance Act on an ex parte basis. *History of the Federal Judiciary: Foreign Intelligence Surveillance Court*, FEDERAL JUDICIAL CENTER, http://www.fjc.gov/history/home.nsf/page/courts_special_fisc.html (last visited Dec. 19, 2013). However, the Department of Justice has had an "almost perfect record" of "obtaining the surveillance warrants and other powers it requested from" FISC. *Id.*

a) *Clapper* Forecloses Judicial Review

The *Clapper* Court rejected the plaintiffs' argument that the Court's strict standing requirements would effectively shield surveillance requests, submitted pursuant to the FISA amendments, from judicial review, since the Foreign Intelligence Surveillance Court (FISC) evaluates each surveillance request.[125] Further, the Court asserted that if the government were to use information obtained through FISC-approved surveillance to prosecute someone, that individual "would certainly have a stronger evidentiary basis" and could thereby "challenge the lawfulness of the acquisition" in federal court.[126]

However, even when the government charges a defendant based on evidence obtained through FISA surveillance, the government may avoid subjecting FISA to constitutional review by relying on alternative evidence.[127] In fact, until recently, the Justice Department's policy has been to withhold the information that FISA surveillance "was an early link in an investigative chain that led to evidence used in court. As a result, none of the defendants knew that they had the right to challenge the warrantless wiretapping law."[128]

The Justice Department may be changing its policy. In October 2013, the "Department for the first time notified a defendant that evidence used against him" had been acquired pursuant to FISA.[129] This change in policy may provide more opportunities for defendants to challenge FISA's constitutionality. However, even if criminal defendants are able to challenge FISA, this challenge would still not adequately address the constitutionality of surveillance that targets individuals who are not suspected of criminal activity.[130]

Several other factors also suggest that *Clapper* may effectively foreclose subjecting FISA to any meaningful constitutional review. First, based on the recitation of the facts in Justice Breyer's dissent, it seems unlikely that any plaintiffs, outside of the criminal justice system, would be more likely targets

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

126. *Id.* at 1154.

127. *See* Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. TIMES (Oct. 26, 2013), *available at* http://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html.

128. *Id.*

129. *Id.*

130. The constitutionality of FISA in either case is outside of the scope of this Note. At this point, it is sufficient to observe that the national security interests involved when a criminal defendant challenges government surveillance render that question a completely separate one from the question posed by the *Clapper* plaintiffs.

of surveillance.[131] Breyer first noted that the plaintiffs' communications with suspected and accused terrorists are exactly the type of information that Congress intended the executive branch to target under FISA.[132] Plaintiffs described in the dissent include: an attorney representing clients who were acquitted of terrorism charges, as well as clients detained at Guantanamo Bay; an attorney representing an international client whom the United States had explicitly threatened; and a human rights researcher who "track[s] down people who were rendered by the CIA to countries where they were tortured."[133] If the targeting of such plaintiffs is not sufficiently certain to establish standing under Article III, the Court has set the bar prohibitively high.

Further, even if a plaintiff had actual evidence that his communications were targeted, the state secrets doctrine would likely prevent him from presenting his evidence in court.[134] Under the state secrets doctrine, the government may bar the disclosure of information upon reasonable showing that such disclosure would undermine national security.[135] Thus, even if plaintiffs do discover invasions of their privacy, "they may not be able to litigate based on their actual knowledge."[136] For example, in *Al-Haramain Islamic Foundation, Inc. v. Bush*, government prosecutors inadvertently gave criminal defendants information revealing that they had been surveillance targets.[137] However, the Ninth Circuit held that the disclosed document was protected by the state secrets doctrine and therefore could not be admitted into evidence or used to establish standing.[138]

b) Verizon Customers' Cases Demonstrate the Dysfunction

Verizon customers, whose status as targets of surveillance is now widely known,[139] may be able to challenge the constitutionality of FISA under current standing rules. Revelations from June 2013 concerning the National

131. *See Clapper*, 133 S. Ct. at 1157–58 (Breyer, J., dissenting).

132. *Id.* at 1158.

133. *Id.* at 1157.

134. Scott Michelman, *Who Can Sue Over Government Surveillance?*, 57 UCLA L. REV. 71, 79–80 (2009).

135. *Id.*

136. *Id.*

137. 507 F.3d 1190, 1194–95 (9th Cir. 2007).

138. *Id.* at 1203.

139. *See, e.g.*, Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (June 5, 2013), *available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Dan Roberts & Spencer Ackerman, *Anger swells after NSA phone records court order revelations*, THE GUARDIAN (June 6, 2013), *available at* http://www.theguardian.com/world/2013/jun/06/obama-administration-nsa-verizon-records.

Security Agency's (NSA's) collection of telephone metadata reveal that the NSA acquired a FISC order "requir[ing] Verizon on an 'ongoing, daily basis' to give the NSA information on all telephone calls in its systems, both within the US and between the US and other countries."[140] The order gave "the government unlimited authority to obtain the data for a specified three-month period."[141] Verizon customers have since brought multiple lawsuits challenging this government action.[142] Even under *Clapper*'s strict standard, there is no question that the plaintiffs were *actually* the targets of surveillance, and therefore they will likely be able to establish an injury-in-fact.[143] Further, since the FISC order is already publicly available, the government may not be able to exclude it from evidence under the state secrets doctrine.[144]

Supporters of the Court's heightened standing requirement in *Clapper* might argue that the Verizon plaintiffs' ability to establish standing demonstrates that *Clapper* did not foreclose judicial review of the FISA amendments. However, this does not demonstrate that the current standing jurisprudence is a workable system. Even if this set of plaintiffs succeeds in establishing standing, the law had to be broken for the necessary information to become available. This demonstrates a precedent so unworkable that citizens have to break the law to gain access to the courts to challenge the legality of potential government infringement of their rights.

c) Entirely Shielding Executive Action from Legislative Review Constitutes an Inappropriate Balance of Powers

Chemerinsky points out that "concern for separation of powers also must include preserving the federal judiciary's role in the system of

140. Greenwald, *supra* note 139.

141. *Id.*

142. Complaint, Klayman v. Obama, No. 1:13-cv-00851 (D.D.C. June 10, 2013), *available at* http://www.freedomwatchusa.org/pdf/130609-Verizon%20Complaint%20Class%20Action.pdf; Complaint, First Unitarian Church of Los Angeles v. NSA, No. 3:13-cv-03287 (N.D. Cal. Sept. 10, 2013), *available at* https://www.eff.org/document/first-unitarian-church-los-angeles-v-nsa-amended-complaint; Complaint, ACLU v. Clapper, No. 13-cv-03994 (S.D.N.Y. June 11, 2013), *available at* https://www.aclu.org/files/assets/nsa_phone_spying_complaint.pdf.

143. *See ACLU v. Clapper – Challenge to NSA Mass Call-Tracking Program,* ACLU, https://www.aclu.org/national-security/aclu-v-clapper-challenge-nsa-mass-phone-call-tracking (last visited Dec. 19, 2013) ("The ACLU does not believe the issue of standing to be a problem in ACLU v. Clapper because of the FISC order showing that the NSA is collecting the telephone records of all Verizon Business customers – including the ACLU.").

144. *But see* J. Steven Gardner, *The State Secret Privilege Invoked in Civil Litigation: A Proposal for Statutory Relief*, 29 WAKE FOREST L. REV. 567, 585 (1994) ("Current standards do not require that information be classified as secret; nor do the standards require that the information not be in the public domain.").

government. Separation of powers can be undermined either by overexpansion of the role of the federal courts or by undue restriction."[145] Current standing jurisprudence for constitutional challenges to government surveillance falls in the latter category, abdicating too much of the Court's power. By creating a nearly insurmountable hurdle to judicial review, the Court displaces a doctrine that has played a key role in supporting the balance of powers since the days of *Marbury v. Madison*.[146]

In crafting the balance of powers framework, and particularly the doctrine of judicial review, the Framers sought to restrict the power of the government as a whole and thereby prevent it from oppressing the people.[147] The judiciary plays an important role this balance by making sure that the actions of the executive and legislative branches do not run afoul of the written imperatives in the Constitution.[148] Without this check "the reservations of particular rights or privileges [in the Constitution] would amount to nothing."[149]

Thus, while the "anti-democratic" judicial branch should not entirely "usurp the powers of the [other] political branches,"[150] using standing doctrine to shield executive and legislative action from judicial review, as the Court did in *Clapper*, also contravenes the purposes of the balance of powers doctrine.

2. Statutory Private-Sector Privacy Litigation

The majority standing jurisprudence in the private-sector context fails for the opposite reason: by choosing not to hear causes of action that the legislature has explicitly sought to authorize through a private cause of action, courts are expanding, rather than limiting, their power at the expense of the legislature.[151] Thus, far from protecting the traditional balance of powers, the "[c]ourt is *sub silentio* inserting into its ostensibly factual

145. CHEMERINSKY, *supra* note 18, at 58.

146. *See* Marbury v. Madison, 5 U.S. 137 (1803); *see, e.g.*, United States v. Nixon, 418 US. 683, 703 (1974) ("Many decisions of this Court, have unequivocally reaffirmed the holding of Marbury v. Madison that '[i]t is emphatically the province and duty of the judicial department to say what the law is."); Cooper v. Aaron, 358 U.S. 1 (1958) (relying on judicial review to overturn Arkansas's refusal to integrate schools).

147. F. Andrew Hessick, *Standing, Injury in Fact, and Private Rights*, 93 CORNELL L. REV. 275, 320 (2008) ("One of the principal functions of the judiciary is to serve as a check on the other branches by ensuring that the other branches do not violate the rights of the people.").

148. *Id.*

149. THE FEDERALIST NO. 78, 469 (Alexander Hamilton).

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

151. Fletcher, *supra* note 47, at 233.

requirement of injury a normative structure of what constitutes judicially cognizable injury that [the legislature] is forbidden to change."[152]

This is especially problematic for privacy law where definitions of harm necessarily evolve with the introduction of new, more intrusive technology.[153] Warren and Brandeis, whose concerns over instantaneous photography instigated the rise of privacy tort law,[154] would be astonished at the rise of Big Data, GPS tracking, and other technologies that represent unprecedented access to individuals' thoughts and actions. Although articulating the harm in this context is not an easy task, the legislature has taken the lead in attempting to define and remedy those harms it sees as the most damaging.[155] In many cases, the legislation also provides a private cause of action, indicating that the legislature envisioned consumers' participation in the law's enforcement. By denying consumers standing absent extraordinary circumstances, the judiciary is circumventing the legislature's attempt to enable private enforcement.

For example, in *Sterk v. Best Buy Stores*,[156] plaintiffs claimed that Best Buy had unlawfully disclosed and retained personally identifiable information in violation of the Video Privacy Protection Act (VPPA).[157] The Northern District of Illinois held that because plaintiffs could not prove concrete economic damages, they did not have Article III standing.[158] However, the type of harm that the VPPA attempts to prevent is not a purely economic one; in most cases the disclosure of video rental records will not result in actual damages.[159] Despite this fact, the legislature chose to specifically provide for liquidated damages to encourage and enable even those unable to prove actual damages to bring suit against violating parties.[160] The fact that the statute explicitly includes such parties indicates that the legislature found

152. *Id.*

153. *See, e.g.*, Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (protecting cable providers' stored data); Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710, 2712 (protecting video rental data); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (restricting collection and use of Internet data pertaining to children); CAN-SPAM Act of 2003, Pub. L. No. 10 8-187 (prohibiting sending classes of unsolicited e-mails).

154. *See* Warren & Brandeis, *supra* note 1, at 195.

155. *See, e.g.*, H.R. REP. No. 108-504, at 2–3 (2004) (describing need for legislation as protecting "individuals [who] have been subjected to a violation of their privacy, only to find it compounded when the pictures or photographs find their way to the Internet.").

156. No. 11 C 1894, 2012 WL 5197901 (N.D. Ill. Oct. 17, 2012).

157. *Id.* at *1.

158. *Id.* at *6–*7.

159. *See* VPPA, 18 U.S.C. §§ 2710–2711 (2012).

160. *See* VPPA, 18 §§ 2710(c)(1)-(2)(A) ("Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court. The court may award . . . not less than liquidated damages in an amount of $2,500.").

non-economic and non-physical harm worthy of vindication. When courts require a separate showing of harm, beyond the harm the legislature impliedly considered important enough to protect, they essentially nullify the legislature's judgment, replacing it with their own—an act that expands, not circumscribes, judicial power.

B. EFFICIENCY

Article III's standing requirement is also said to "serve judicial efficiency by preventing a flood of lawsuits by those who have only an ideological stake in the outcome."[161] This goal is not convincing in the case of lawsuits against the government. Even in the private sector, the Ninth Circuit rule likely does not substantially affect judicial efficiency. However, granting access to a larger number of plaintiffs may have a negative impact on industries that work with large amounts of consumer data.

1. Constitutional Challenges

As a primary matter, under the doctrine of collateral estoppel, the Court will only need to make a decision on the constitutionality of a government action, such as a particular surveillance procedure, once: "Under collateral estoppel, once a court has decided an issue of fact or law necessary to its judgment, that decision may preclude relitigation of the issue in a suit on a different cause of action involving a party to the first case."[162] Thus, if the Court had ruled on the merits in *Clapper*, it would not have to rule on the same issue again against a different set of plaintiffs. In fact, denying standing in *Clapper* may have been the Court's least efficient option, as now that Verizon customers have more evidence to help them establish standing, in the form of a FISC order authorizing the NSA to target their phone conversations, multiple parties are challenging FISA's constitutionality for a second time.[163]

Moreover, the Supreme Court has repeatedly stated that efficiency justifications do not prevail over important constitutional considerations: "[T]he Constitution recognizes higher values than speed and efficiency. . . . [The Bill of Rights was] designed to protect the fragile values of a vulnerable citizenry from the overbearing concern for efficiency and efficacy . . . ."[164]

---

161. CHEMERINSKY, *supra* note 18, at 58.

162. Allen v. McCurry, 449 U.S. 90, 94 (1980).

163. *See supra* note 142.

164. Stanley v. Illinois, 405 U.S. 645, 656 (1972); *see also* Reed v. Reed, 404 U.S. 71 (1971) (holding that efficiency concerns are not sufficient to overcome even rational basis test).

Judicial efficiency concerns therefore do not justify the Court's decision in *Clapper*.

2. Private-Sector, Statutory Suits

Even in the private-sector, statutory context, traditional efficiency arguments, which focus on the burden on the court system, do not hold much weight. The Supreme Court has expressed concern that forgoing a stringent injury-in-fact standard would result in an onslaught of new litigation that would hinder the administration of justice. For example, Justice Powell's concurrence in *United States v. Richardson* expressed concern that "we risk a progressive impairment of the effectiveness of the federal courts if their limited resources are diverted increasingly from their historic role . . . ."[165]

However, in the privacy context, the small amount of potential recovery per plaintiff and large costs of litigation often compel plaintiffs to organize into class action lawsuits. Thus, for example, even though Facebook's alleged violation of California's right of publicity law in *Fraley v. Facebook* affected 150 million users,[166] the federal court system did not have to deal with 150 million lawsuits. Rather, plaintiffs consolidated their claims into a single lawsuit, transferring the burden and administrative headache from the court system to the lead plaintiff and his attorneys, while also allowing plaintiffs—who might not otherwise consider the value of filing an individual lawsuit worth the cost and effort—to recover for the harm inflicted upon them.

Although class actions are relatively efficient for the court system, they may result in astronomical judgments for minor statutory violations, which may place a heavy burden on companies that collect and use large amounts of consumer data.[167] Even a minor violation, when multiplied by millions of affected users can result in a "multi-*billion* dollar statutory damages claim—without [any] class member having suffered any [economic] injury from the practice or act at issue."[168]

---

165. United States v. Richardson, 418 U.S. 166, 192 (1974) (holding that plaintiffs could not establish standing as a taxpayer by alleging that a government agency had wasted taxpayer money).

166. *Judge Approves $20 million settlement in Facebook class-action lawsuit*, THE RAW STORY (Aug. 26, 2013), http://www.rawstory.com/rs/2013/08/26/judge-approves-20-million-settlement-in-facebook-class-action-lawsuit/.

167. *See* Brief of Amicus Curiae Facebook Inc., LinkedIn Corp., Yahoo! Inc., and Zynga Inc. in Support of the Petitioners, First Am. Fin. Corp. v. Edwards, 132 S. Ct. 2536 (2011) (No. 10-708), 2011 WL 3857211, at *17.

168. *Id.* at *3. *See, e.g.*, Cory L. Andrews, *Two Cheers For Judicial Actions In Facebook, Ebay Class Action Settlements*, FORBES (Aug. 29, 2013), http://www.forbes.com/sites/wlf/2013/08/29/two-cheers-for-judicial-actions-in-facebook-ebay-class-action-settlements/ (describing $20 million Facebook settlement regarding the use of "likes" to advertise to friends through

In addition to the danger posed to individual defendant companies, excessive litigation may have a negative impact on the economy by discouraging companies from innovating in fields that rely on consumer data or by tying up too much corporate energy and capital in litigation.[169] Thus, courts may wish to protect defendants, and industry in general, by reducing the overall number of lawsuits using a stricter definition of harm than the legislature intended.

Nonetheless, plaintiffs' and plaintiffs' attorneys' inclinations towards frivolous litigation may not be as strong as some fear. Since a class action attorney and lead plaintiff will both "need to invest his or her time and money to bring a civil suit; [this] will further help to limit litigation to plaintiffs with significant personal interest in the matter."[170] Despite the potential to receive a lucrative settlement or judgment, lead plaintiffs and their attorneys may not be willing to invest this amount of time and energy in claims that are sure losers.[171]

Further, legislatures are likely aware of the potential burden of excessive litigation and are capable of managing the floodgates by fine-tuning the legislation itself. The legislature's ability to craft nuanced and context-specific standing and substantive requirements makes it more capable of reacting to or preempting negative economic impacts and emerging technologies than a one-size-fits-all standing requirement.

---

sponsored stories, and noting that plaintiffs suffered no economic injury); Debra Cassens Weiss, *Netflix Notifies Customers of Class Action Settlement; Privacy Groups Will Benefit*, ABA JOURNAL (Aug. 1 2012), http://www.abajournal.com/news/article/netflix_notifies_customers_of_class_action_settlement_privacy_groups_will_b/ (describing $9 million Netflix settlement for retaining customer data more than one year after cancelling service). This is especially true in situations where defendants may not even be particularly culpable. For example, the unauthorized access to a large number of user accounts may be caused by the website's poor security, but it could also be caused by a phishing scheme, wherein a malicious third party tricks users into disclosing their passwords, without any actual breach of the defendant's software.

169. In a study titled "The Impact of U.S. Internet Privacy Regulations on Early-Stage Investment," Booz & Co. "found that uncertain, potentially large damage awards, make[] early-stage investors uncomfortable with investing in that space." BOOZ & CO., THE IMPACT OF U.S. INTERNET PRIVACY REGULATIONS ON EARLY-STAGE INVESTMENT: A QUANTITATIVE STUDY 22 (2011), *available at* http://www.booz.com/media/file/BoozCo-Impact-US-Internet-Privacy-Regulations-Early-Stage-Investment.pdf.

170. Patricia Cave, Note, *Giving Consumers a Leg to Stand On: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits*, 62 CATH. U. L. REV. 765, 793 (2013).

171. *But see* AT&T Mobility LLC v. Conception, 131 S. Ct. 1740, 1752 (2011) (noting "even a small chance of a devastating loss" may compel defendants to settle even obviously non-meritorious lawsuits).

For example, a legislature could limit the flood of data breach litigation—while still giving plaintiffs the opportunity to protect themselves—by requiring that plaintiffs purchase credit-monitoring services as an element of the cause of action itself.[172] The legislature could thereby "ensure that plaintiffs will not assert broad and unfounded claims based on a hypothetical fear of identity theft."[173] Further, by limiting recovery to the cost of credit-monitoring services, the legislature could "guarantee[] that recovery is limited to actual expenses incurred by a plaintiff because of a business's noncompliance with regulatory standards for data security management."[174]

The legislature could also limit liability by fundamentally changing the nature of the underlying cause of action. For example, Professor Jane K. Winn has suggested that security breach notification laws would more effectively reduce security breaches if the legislature replaced the current strict liability regime with a statutorily defined negligence standard.[175] Sanctions could be tied to the "wrongfulness of the conduct that led to the breach," rather than "the volume of the data exposed,"[176] and would therefore preclude large judgments or settlements for minor statutory violations.

Thus, while the Ninth Circuit rule may initially create negative economic impacts, a judicially determined standing requirement is not the only way to limit frivolous litigation. In fact, the legislature has more tools at its disposal to control the number of plaintiffs who have access to the courts.

C. IMPROVING JUDICIAL DECISION-MAKING & ENSURING FAIRNESS

Finally, proponents of a strict standing requirement argue that the requirement improves judicial decision-making and ensures fairness.[177] Strict standing requirements, it is said, "improve judicial decision-making by ensuring that there is a specific controversy before the court and that there is an advocate with a sufficient personal concern to effectively litigate the

172. Cave, *supra* note 170, at 793.

173. *Id.*

174. *Id.*

175. Jane K. Winn, *Are "Better" Security Breach Notification Laws Possible?*, 24 BERKELEY TECH. L.J. 1133, 1160 (2009).

176. *Id.* at 1159–60.

177. The "fairness" justification is typically applied when referring to prudential standing, rather than Article III standing. *See, e.g.*, Singleton v. Wulff, 428 U.S. 106, 113 (1976) (holding that fairness may dictate "hesitat[ion] before resolving a controversy, even one within their constitutional power to resolve"); Miller v. Albright, 523 U.S. 420, 422 (1998) ("This Court applies a presumption against third-party standing as a prudential limitation on the exercise of federal jurisdiction."). However, for the sake of thoroughness, this Note addresses any potential relevance to Article III standing here.

matter."[178] The injury-in-fact requirement is said to encourage fairness "by ensuring that people will raise only their own rights and concerns and that people cannot be intermeddlers trying to protect others who do not want the protection offered."[179] To frame this justification in a different way, standing encourages fairness by "ensur[ing] that the legal remedies of primary victims of wrongful conduct will not be usurped by persons trivially or not at all harmed by the wrong complained of."[180]

Both these justifications present widely recognized problems. In some cases the particular plaintiff bringing suit may have little bearing on the accuracy or fairness of a case's outcome, as "some cases present pure questions of law in which the factual context is largely irrelevant."[181] For example, if a city government were to entirely ban abortions, the constitutional question of whether such a policy violated citizens' due process right to decisional privacy would not depend much on who was suing the city.[182] Further, "the insistence on a personal stake in the outcome of the litigation is a very uncertain guarantee of high quality advocacy."[183] For example, a pro se applicant may be fully invested in his case but may lack the skills required to effectively present it. In contrast, a top litigator may be so skilled at presenting a case that it does not matter that the facts do not relate to him personally.[184] Finally, "standing requirements might be quite unfair if they prevent people with serious injuries from securing judicial redress."[185]

178. CHEMERINSKY, *supra* note 18, at 58; *see also* Baker v. Carr, 369 U.S. 186, 204 (1962) (holding that plaintiff must allege "such a personal stake in the outcome of the controversy as to assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends for illumination of difficult and constitutional questions").

179. CHEMERINSKY, *supra* note 18, at 59.

180. Am. Bottom Conservancy v. U.S. Army Corps of Eng'rs, 650 F.3d 652, 656 (7th Cir. 2011); *see also* Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 473 (1982) (quoting United States v. SCRAP, 412 U.S. 669, 687 (1973)) ("The federal courts have abjured appeals to their authority which could convert the judicial process into 'no more than a vehicle for the vindication of the value interests of concerned bystanders.'").

181. CHEMERINSKY, *supra* note 18, at 59.

182. *Id.* It is possible to foresee a situation where a party who is actually in favor of the law brings a suit against it and then does a poor job of representing the case in order to preclude others from challenging the law. However, more interested parties may be able to counteract such a scheme by joining the lawsuits as co-plaintiffs. Perhaps even more importantly, it seems overkill to deny legal access to large swaths of good-faith plaintiffs in order to deter the seemingly small possibility of a bad-faith plaintiff.

183. *Id.*

184. *Id.* Justice Scalia agrees, explaining that:

> [T]he doctrine is remarkably ill designed for its end. Often the very best adversaries are national organizations such as the NAACP or the American Civil Liberties Union that have a keen interest in the abstract

The fact that most privacy litigation is brought in the form of class action suits provides special context to the discussion of fairness and decision-making quality. The class certification requirements embodied in Federal Rules of Civil Procedure Rule 23(a)(3)—"the claims or defenses of the representative parties are typical of the claims or defenses of the class"—and Rule 23(a)(4)—"the representative parties will fairly and adequately protect the interests of the class"—already serve as a protection to make sure that "there is an advocate with a sufficient personal concern to effectively litigate."[186] Further, plaintiffs have an incentive to find such a class representative as, even without stringent standing requirements, the outcome of a class action might vary a lot depending on who serves as lead plaintiff.

The difference in characterization of the affected plaintiffs by the majority and the dissent in *Clapper* demonstrates the importance of finding the best class representatives. The *Clapper* majority described plaintiffs merely as "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."[187] The dissent, however, focused on certain lead plaintiffs, who may have had particularly strong cases.[188] As discussed above, the dissent describes an attorney representing clients who were acquitted of terrorism charges, an attorney representing an international client who was explicitly threatened by the United States, and a human rights researcher who "track[s] down people who were rendered by the CIA to countries where they were tortured."[189] This difference in characterization may have resulted from the majority and dissent viewing different lead plaintiffs as representatives of the class.

Thus, to succeed under a privacy class action lawsuit, plaintiffs are already constrained to select a lead plaintiff who has "sufficient personal concern to effectively litigate"[190] and who can present a specific and persuasive case.

> question at issue in the case, but no 'concrete injury in fact' whatever. Yet the doctrine of standing clearly excludes them . . . .

Scalia, *supra* note 119, at 891.

185. CHEMERINSKY, *supra* note 18, at 59.

186. *See id.* at 58. To the extent that unnamed plaintiffs are not able to control who represents them as lead plaintiff in a class action lawsuit, they do, at least, have the ability to opt out and bring their own class action.

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

188. *Id.* at 1156–57 (Breyer, J., dissenting).

189. *Id.*

190. CHEMERINSKY, *supra* note 18, at 58.

D. A PROPOSED FIFTH GOAL: FLEXIBILITY

Perhaps most importantly, the *Edwards* standard does a better job of drawing a line that grants access to worthy plaintiffs while protecting defendants and courts from unworthy plaintiffs and cases. Current standing jurisprudence represents an understanding that the definition of injury-in-fact must apply in the same way to every cause of action.[191] Judges are thus required to draw a single line over a varied and complicated legal landscape. Courts therefore determine standing based on the extension of or analogy to already-established, acceptable types of harm, rather than identifying the proper balance of access for a given area of law. This is a particularly strained process in the privacy context, where the types of harm at issue are substantially different from traditional types of harm. As a result, the application of the injury-in-fact requirement is unpredictable—it is difficult to predict what type of extension or analogy a court will use. Worse still, it can never be precise enough to achieve the desired effect of granting access to worthy plaintiffs while barring unworthy claims.

The underlying cause of action for any given case already represents a sorting of worthy and unworthy claims on a more context-specific level. In relying on the harm implicated by the underlying cause of action, the Ninth Circuit's *Edwards* standard therefore not only eliminates duplicate work but also achieves a more narrowly tailored method of sorting.

1. Applying the Edwards *Standard to Constitutional Context*

The problem with current standing precedent for cases challenging the constitutionality of government surveillance is not simply that it prevents too many people from challenging government actions; the problem is that the harm required to challenge government action is not coextensive with the harm that the Constitution seeks to protect.

The Bill of Rights addresses a series of implied harms that the Framers of the Constitution found to be particularly pernicious. For example, the Framers created and ratified the Fourth Amendment in response to the colonial general warrants and writs of assistance, which gave colonial governments unlimited authorization to "search a man's house, his person, his papers, and his effects."[192] Yet, even the most basic physical search of a citizen's property does not necessarily result in physical or economic damage.

---

191. *See* Fletcher, *supra* note 47, at 223 ("As currently constructed, standing is a preliminary jurisdictional requirement, formulated at a high level of generality and applied across the entire domain of law.").

192. Olmstead v. United States, 277 U.S. 438, 463 (1928).

Clearly though, the inclusion of such a prohibition in the Constitution indicates that the Framers sought to protect more than the physical and monetary. Because the Framers did not elaborate on the precise philosophical nature of the harm that inspired the Bill of Rights—nor could they predict the ways in which society would develop to recognize certain harms in light of advancing technology—the best way to analyze whether a plaintiff has been harmed in the way the Framers sought to prevent is by analyzing the substantive aspects of the plaintiff's case—that is, applying the constitutional prohibitions to the facts of the plaintiff's claim.[193]

Because the Court held that the *Clapper* plaintiffs failed to establish standing, it remains unclear whether the FISA amendments violate the Constitution in the way that the *Clapper* plaintiffs claimed. Regardless of the answer to this question, it is troubling that the Court considered whether there was injury-in-fact without first looking at what would constitute injury under the First and Fourth Amendments. Unless the standing question of harm is merged with the harm implicated by the relevant portion of the Constitution, there is a chance that some people who have been harmed in a way that is constitutionally actionable will not be able to challenge the government, despite the Framers' intent to protect them.

2. *Evaluating* Edwards *in the Statutory Context*

In the statutory context, the court's exercise of power in asserting its definition of harm over that of the legislature not only upends the traditional balance of power, it also circumvents the best interests of the people by potentially excluding plaintiffs the legislature found to be worthy of protection. Privacy advocates have argued that "[p]rivacy is a concept too integral to the person and a right too essential to freedom to allow its manipulation to support just those ideas the government prefers."[194] However, to the extent that a government body has to define harm in order to ensure its protection, the legislature is in the best position to do so.

While the judiciary's role is important for enforcing a constitutional minimum, when the legislature enacts legislation that rises above this minimum, its definition of harm should be given deference for two reasons. First, since the legislature is the most democratic branch, its definitions of harm are the most likely to reflect the types of harm that the citizenry views as worthy of protecting. Secondly, "[i]n circumstances involving dramatic

193. *See* Fletcher, *supra* note 47, at 224 ("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.").

194. Sorrell v. IMS Health, Inc., 131 S. Ct. 2653, 2672 (2011).

technological change," the legislature is best "suited to gauge changing public attitudes, to draw detailed lines, and to balance privacy and [other interests] in a comprehensive way."[195] As Professor Orin Kerr explains: "Legislatures can enact comprehensive rules based on expert input and can update them frequently as technology changes. As a result, legislatures can generate more nuanced, balanced, and accurate privacy rules when technology is in flux."[196]

The *Edwards* rule gives legislatures the power to define and redefine actionable privacy harms without hampering causes of action with less adaptive precedential requirements. In other words, as society and technology evolve together, the *Edwards* rule does the best job drawing a line of access to the court system that is closely tailored to the harms that society feels should be protected.

V. CONCLUSION: HOW TO TAILOR STANDING

The injury-in-fact requirement poses a difficult problem in the privacy context, as the appropriate definition of harm may depend on the type of privacy loss in question. Because current precedent requires courts to determine standing without referring to the underlying causes of action, it is unclear how judges should determine what type of harm applies.

Porting the Ninth Circuit's standard to claims arising under the Constitution and under statutes, even those without liquidated damages, provides a clearer standard for judges when determining whether plaintiffs have suffered an injury-in-fact. In both cases, a court would simply grant standing if it determines that the defendants violated the underlying cause of action.[197] In the constitutional law context, this would avoid scenarios like *Clapper*, where the standing requirement upended the balance of powers by shielding the executive branch's surveillance programs from constitutional review. The Ninth Circuit's standard may also be more efficient because the

195. United Stated. v. Jones, 132 S. Ct. 945, 964 (2013) (Alito, J., conccurring).

196. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 807–08 (2004).

197. The courts would still need to require some nexus between the violation and the plaintiffs. Even in *Edwards* the court did not go so far as to extend standing to all citizens. The plaintiffs were First American's customers at the time the violation occurred. Edwards v. First. Am. Fin. Corp., 610 F.3d 514, 516 (9th Cir. 2010). The nature of this nexus lies beyond the scope of this Note. Suffice it to say that the nexus requirement would not pose as high of a barrier as the majority of jurisdictions' judicially defined injury-in-fact requirement.

Court can decide once on a constitutional issue without having to hear different plaintiffs' repeated attempts to establish standing.[198]

In the statutory law setting, the Ninth Circuit's approach better serves the goal of balancing the three branches of government because it does not give the judicial branch the power to completely override the legislature's conceptualization of harm and attempted solutions. Although the Ninth Circuit's approach may result in greater exposure to liability for those industries that deal with consumer information, the legislature could limit liability by imposing other requirements—for example, proof of actual damages—as an element of a particular underlying claim.

Further, merging standing with substance provides more clarity, thereby encouraging settlement and rendering the litigation process *more* efficient. When the law is clearer, parties can better evaluate the strength of their respective cases and can therefore negotiate more knowledgably. With a shared understanding of the contours of the law, it would likely be easier for the parties to reach settlements, and the resulting agreements would likely include more predictable and reasonable settlement amounts. Settlements that accurately reflect the relative strength of the parties' cases are efficient for everyone. They reduce the court's role and the burden on the judicial system. They also save plaintiffs and defendants the costs of litigation.

The injury-in-fact requirement, as it stands in the majority of jurisdictions, introduces more uncertainty, as it premises access on an opaque and malleable process of defining "harm." When the law is less clear, parties may be more inclined to continue litigating, or defendants may choose to defend against a small probability of a larger judgment by settling for much more than a claim is worth. Thus, in this respect, current standing doctrine undermines the policy goal of efficiency.

Moreover, to the extent that increasing access to privacy causes of action would have a negative impact on the economy, the threat of suit may force the economy, and the technology industry in particular, to evolve such that companies are more careful about their choices of what kinds of data to collect. For example, it is currently very common for companies to collect social security numbers. The benefit the company derives from collecting this information pales in comparison to the devastating impact such information could have on consumers if the information is exposed.[199] In order to

198. *See supra* note 142.

199. *See, e.g.*, Barbara Kiviat, *Guarding Your Social Security Number*, TIME (Dec. 4, 2007) http://content.time.com/time/business/article/0,8599,1690827,00.html ("Their computer system wouldn't let them process orders without a Social Security number, but if I called Verizon directly maybe they could do something different."); *id.* (describing a 1.5 hour-long

minimize the likelihood of data misappropriation, companies may choose to limit the types of information gathered to those that are narrowly tailored to their needs. Thus, even if the *Edwards* standard is less efficient in the short-term, it may lead to corporate practices that are not only more efficient in the long run, but also more protective of consumer privacy.

Although the injury-in-fact requirement for Article III standing is intended to serve as a tool for withholding court access from claims that are not socially beneficial, when the potential injury in question is a privacy harm, injury-in-fact is a difficult tool to utilize. Fortunately, it is also an unnecessary one. As the above analysis demonstrates, requiring judges to determine whether or not a plaintiff has suffered a privacy harm without looking at the definition implicated by the underlying cause of harm more often than not cuts against the goals of standing doctrine and leaves a great deal of confusion in its wake. The Ninth Circuit rule exemplifies a superior approach for adjudication of constitutional and statutory privacy issues.

ordeal trying to find a way around Verizon's requirement that people sign up for cell service with a Social Security number and concluding that all Verizon needed was two forms of identification, indicating that Verizon could perform the same function through less intrusive means); Adam Levin, *5 Places Where You Should Never Give Your Social Security Number*, HUFFINGTON POST (Mar. 28, 2013), http://www.huffingtonpost.com/adam-levin/identity-theft_b_2967679.html ("[M]any companies collect Social Security numbers they don't need because they're operating on autopilot. They've always done it, and their colleagues at other companies do it, so the practice continues and spreads on the strength of simple, dumb inertia.").