2015

Online Data Breaches, Standing, and the Third-Party Doctrine

Adam Lamparello
Indiana Tech Law School

ONLINE DATA BREACHES, STANDING, AND THE THIRD-PARTY DOCTRINE

Adam Lamparello†

TABLE OF CONTENTS

INTRODUCTION

When citizens call a loved one from a cell phone, use a credit card to purchase a New York Times bestseller on Amazon, or type in a social security number to apply for an online loan, they surrender all privacy rights to that information.[1] These citizens must rely on a merchant or service provider to protect this information from being unlawfully accessed by third parties.[2] In the unfortunate event of an online data breach, some citizens may discover unauthorized charges on their credit cards, and may be forced, at substantial cost, to close all of their online accounts, repair damage to their credit score, and take other measures to prevent future harm.[3] Citizens may find it difficult, however, to recover

† Assistant Professor of Law, Indiana Tech Law School.

1 *See, e.g.*, United States v. Miller, 425 U.S. 435, 446 (1976) (holding that consumers forfeit their privacy rights in financial information that is given to a bank teller); Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (upholding the use of a pen register to monitor outgoing calls from a suspect's residence).

2 *See, e.g.*, *Online Data Breach Reports Increase*, ACA INTERNATIONAL, http://www.acainternational.org/creditors-online-data-breach-reports-increase-31825.aspx (last visited Mar. 3, 2015) (discussing the prevalence of online data breaches and the resulting misappropriation of personal information).

3 Kimberly Kiefer Peretti, *Data Breaches: What the Underground World of 'Carding' Reveals*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 375, 379 (2009). Peretti further states:

> The compromise of credit and debit card account information most often results in the

mitigation damages and often cannot sue a merchant or provider for the invasion of privacy that online data breaches cause.[4]

Specifically, the standing, third party, and reasonable expectation of privacy doctrines limit consumers' ability to recover costs associated with preventing future harm from online data breaches, which can include credit and internet monitoring services, identity theft insurance and/or data breach risk mitigation services.[5] Indeed, consumers are often unable to recover mitigation damages for purchasing services like those mentioned above because the prevention of future harm is not considered sufficiently imminent to confer standing.[6]

Additionally, courts typically reject claims based on an invasion of privacy theory.[7] This is due in part to the third-party doctrine, which states that citizens surrender all privacy rights in information voluntarily conveyed to a third party, and thus must assume the risk that such information will be knowingly or inadvertently conveyed to others, including the government.[8] As a result, when a merchant's or provider's server is hacked, consumers do not suffer an actual, concrete, and cognizable legal "injury" and therefore lack Article III standing to sue

---

> type of identity theft referred to as "account takeover," which involves fraud on existing financial accounts. Account takeovers occur, for example, when a criminal uses a stolen credit card number to make fraudulent purchases on an existing credit line. Account takeovers are the more common type of identity theft, in contrast to a second type of identity theft referred to as "new account creation." New account creations involve the fraudulent creation of new accounts, for example, when a criminal uses stolen data to open a bank or credit card account in someone else's name.

Id.

[4] *See, e.g.*, Douglas H. Meal, *Private Data Security Breach Litigation in the United States*, 2014 WL 10442 at *3 (January 2014). Courts are reluctant to reward emotional distress or privacy damages for online data breaches:

> Plaintiffs have . . . alleged that the exposure of their information injured them by causing emotional injury, such as anxiety or stress, or a loss of privacy. Neither theory appears to have been embraced by the courts. Courts have generally found allegations of emotional distress to be insufficient to state a claim for relief. As to loss of privacy, some courts have held that a loss of privacy constitutes actionable harm only if there is an intentional or egregious invasion of privacy not present in actions against breached companies, while others have rejected such claims of harm outright.

Id. (citing Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1055 (E.D. Mo. 2009); *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 132–33 (D. Me. 2009), *aff'd in part*, *rev'd in part sub nom*, Anderson v. Hannaford Bros. Co., 659 F.3d 151, 166–67 (1st Cir. 2011); Randolph v. ING Life Ins. & Annuity Co., 973 A.2d 702, 711 (D.C. 2009); Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1127–28 (N.D. Cal. 2008)).

[5] *See, e.g.*, *Once Again, Clapper Defeats Data Breach Class Action*, DATA PRIVACY MONITOR (Feb. 14, 2014) http://www.dataprivacymonitor.com/online-privacy/once-again-clapper-defeats-data-breach-class-action.

[6] *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 657 (S.D. Ohio 2014) (holding that the plaintiffs could not recover costs associated with preventing future harm).

[7] *See* Meal, *supra* note 4, at *3 ("Plaintiffs have . . . alleged that the exposure of their information injured them by causing emotional injury . . . or a loss of privacy. Neither theory appears to have been embraced by courts").

[8] *See* United States v. Miller, 425 U.S. 435, 443 (1976).

on privacy grounds.[9]

This Essay argues that, in the context of online data breaches, these doctrines hinder consumers from receiving full monetary compensation and do not adequately safeguard privacy rights. For example, courts frequently dismiss consumers' suits against online service providers for lack of standing, which results in consumers bearing the cost for damages that the providers were in a position to prevent. This Essay argues that the Supreme Court should relax the standing doctrine's "imminent harm" requirement and permit consumers to sue providers for mitigation damages. In addition, the Court should abandon the long-standing principle that citizens lose all privacy protections in personal information voluntarily given to third parties. Relatedly, the Court should modify the two-pronged framework set forth in *Katz v. United States*[10] and focus exclusively on whether there exists an objective societal expectation of privacy in personal information that third parties unlawfully access.[11] This approach will ensure that consumers are fully compensated for the direct and foreseeable harms that online data breaches cause, and provide incentives for private companies to adopt stringent policies that minimize the risk of future breaches.

I. INSUFFICIENT LEGAL PROTECTIONS FOR CONSUMERS

A. *The Third-Party Doctrine's Impact on Privacy Rights and Standing*

In *Katz v. United States*, the Court held that Fourth Amendment protections apply only where an individual has a subjective expectation of privacy in the data or objects that are subject to a search, and where "society is prepared to recognize [that expectation] as 'reasonable.'"[12] Although breaches of a private company's server do not implicate the Fourth Amendment,[13] the third-party doctrine is an outgrowth of *Katz* and reflects the Court's view that citizens do not retain privacy rights when they knowingly and intentionally surrender information to third parties.

The third-party doctrine is a product of pre-digital era case law. In

---

9 *See, e.g.*, Lexi Rubow, *Standing in the Way of Privacy Protections: The Argument for a Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action*, 29 BERKELEY TECH. L.J. 1007, 1010 (2014).

10 389 U.S. 347, 361 (1967).

11 *See id.*

12 *Id.*

13 The Fourth Amendment only applies to state action; merchants and providers are not considered state actors. *See, e.g.*, Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614 (1989) (noting that "the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative").

United States v. Miller, the Court held that citizens have no expectation of privacy in financial information "voluntarily conveyed to [] banks and exposed to their employees in the ordinary course of business."[14] The Court's holding rested on the notion that individuals must assume the risk that information voluntarily provided to third parties will be disclosed to others:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government . . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[15]

Thus, because "the depositor 'assumed the risk' of disclosure . . . it would be unreasonable for him to expect his financial records to remain private."[16]

Similarly, in *Smith v. Maryland*, the Court upheld law enforcement's use of a pen register to monitor outgoing calls from a suspect's residence.[17] The *Smith* Court relied on *Miller*, holding that by "expos[ing] . . . information to its equipment in the ordinary course of business[, the suspect] assumed the risk that the company would reveal to police the numbers he dialed."[18] The Court also emphasized that "pen registers do not acquire the contents of communications,"[19] and that "people in general [do not] entertain any actual expectation of privacy in the numbers they dial."[20] Thus, "[a]lthough [the suspect's] conduct

---

14 United States v. Miller, 425 U.S. 435, 442 (1976).

15 *Id.* at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971) (plurality opinion); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427, 439 (1963)). In his dissent, in *Smith v. Maryland*, Justice Marshall stated:

> The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts . . . . Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society. Particularly given the Government's previous reliance on warrantless telephonic surveillance to trace reporters' sources and monitor protected political activity, I am unwilling to insulate use of pen registers from independent judicial review.

442 U.S. 735, 751 (1979) (Marshall, J., dissenting) (citations omitted).

16 *Smith*, 442 U.S. at 744 (discussing *Miller*).

17 *See id.* at 745–46.

18 *Id.* at 744.

19 *Id.* at 741.

20 *Id.* at 742. The Court explained:

> Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They

may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed."[21] In his dissent, Justice Marshall argued that "[t]hose who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[22]

Recently, however, the Court has called into question the continuing viability of the third-party doctrine. In *United States v. Jones*,[23] the Court held that the government's use of a GPS tracking device to monitor a suspect's whereabouts on public roads for twenty-eight days constituted a search under the Fourth Amendment.[24] Although the Court was divided over whether the search was an unlawful trespass or an infringement of privacy, five Justices suggested that the length of the surveillance violated a *societal* expectation of privacy, notwithstanding the fact that the suspect's vehicle was traveling on public roads and readily observable.[25] Furthermore, in her concurrence, Justice Sotomayor directly questioned the validity of the third-party doctrine, including "the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[26]

Likewise, in *Riley v. California*,[27] the Court held that, in the absence of exigent circumstances, law enforcement may not search the contents of a suspect's cell phone without a warrant and probable cause.[28] The Court relied on the fact that, unlike finite objects such as plastic containers or crumpled cigarette packs, cell phones store volumes of private information, such as photographs, financial documents, and emails.[29] In both cases, the Court could have applied the third-party doctrine and held that citizens have no expectation of privacy in their public movements or outgoing calls. By doing the

---

> disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.

Id. at 741 (quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)).

[21] *Id.* at 743 (stating "even if he did [have a subjective expectation of privacy], his expectation was not 'legitimate'").

[22] *Id.* at 749 (Marshall, J., dissenting).

[23] 132 S. Ct. 945 (2012).

[24] *See id.* at 949 (plurality opinion).

[25] *Id.* at 964 (Alito, J., concurring) ("society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period").

[26] *Id.* at 957 (Sotomayor, J., concurring).

[27] 134 S. Ct. 2473 (2014).

[28] *Id.* at 2495.

[29] *Id.* at 2491 ("A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.").

opposite and focusing on a societal—rather than subjective—expectation of privacy, the Court suggested that the third-party doctrine may be on its last legs.

The federal courts, however, continue to be divided on whether the third-party doctrine applies to digital-era searches. In *Klayman v. Obama*,[30] the United States District Court for the District of Columbia held that the National Security Agency's (NSA) metadata collection program constituted a search under the Fourth Amendment.[31] The district court refused to apply the third-party doctrine, holding that "the *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones."[32] Among those distinctions was the sheer volume and breadth of the metadata collection program.[33] As the district court explained, it is one thing for citizens to assume that "phone companies [] occasionally provide information to law enforcement," but quite another to expect "all phone companies to operate . . . a joint intelligence-gathering operation with the Government."[34] Conversely, in *ACLU v. Clapper*,[35] the United States District Court for the Eastern District of New York held that the third-party doctrine negated any expectation of privacy for outgoing cell phone calls.[36] To date, no cases on the Court's docket directly address the third-party doctrine's continuing validity.[37]

---

30 957 F. Supp. 2d 1 (D.D.C. 2013).

31 *Id.* at 32.

32 *Id.* at 37.

33 *Id.* at 35–36.

34 *Id.* at 33 (monitoring calls from a single suspect's residence "in no way resembles the daily, all-encompassing, indiscriminate dump of phone metadata that the NSA now receives as part of its . . . Metadata Program").

35 959 F. Supp. 2d 724 (E.D.N.Y. 2014)

36 *Id.* at 749; *see also* United States v. Moalin, No. 10 Cr 4246(JM), 2013 WL 6079518, at *7–8 (S.D. Cal. Nov. 18, 2013) (applying *Smith* to uphold the NSA's metadata collection program); United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012) (individuals have no expectation of privacy in information transmitted from a pay-as-you-go cell phone); *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 146 (E.D.N.Y. 2013) ("[g]iven the notoriety surrounding the disclosure of geolocation data . . . cell phone users cannot realistically entertain the notion that such information would (or should) be withheld from federal law enforcement agents searching for a fugitive").

37 *But see* Patel v. City of Los Angeles, 738 F.3d 1058 (9th Cir. 2013), *cert. granted*, City of Los Angeles v. Patel, 135 S. Ct. 400 (2014). In *Patel*, the Court will address whether: (1) facial challenges based on the Fourth Amendment are permissible; and (2) warrantless searches of a hotel's guest registry violate a hotel owner's reasonable expectation of privacy and thus require a warrant and probable cause. Professors Adam Lamparello and Charles E. MacLean filed a brief in this case arguing that the Court should modify the third-party doctrine and hold that searches of hotel guest registries violate the hotel guests' expectation of privacy. Although the Court is only focusing on the privacy rights of hotel owners, a credible argument can be made that these searches violate the hotel guests' privacy rights. *See* Brief for Adam Lamparello & Charles E. MacLean as Amici Curiae Supporting Respondents, City of Los Angeles v. Patel, No. 13-1175 (argued Mar. 3, 2015), *available at* http://sblog.s3.amazonaws.com/wp-

B. *The Third-Party Doctrine's Impact on Standing and the Preclusive Effect of the Imminent Harm Requirement*

The third-party doctrine makes it difficult, if not impossible, for plaintiffs to claim that online data breaches violate a reasonable expectation of privacy. The standing doctrine's "imminent harm" requirement also prevents citizens from recovering costs associated with preventing future harm.[38]

By way of background, the standing doctrine originates from the "case or controversy" requirement in Article III of the Constitution.[39] Standing focuses on "access apart from the merits of the controversy,"[40] and addresses "whether a specific person is the proper party to bring a matter to the court."[41] Under the Supreme Court's current jurisprudence, to establish standing a plaintiff must show that an injury is "(1) concrete, particularized, and actual or imminent; (2) fairly . . . trace[able] to the challenged action; and (3) redress[able] by a favorable decision."[42] Accordingly, a plaintiff may not assert a "generalized grievance," that reflects the "harm . . . to every citizen's interest in proper application of the Constitution and laws" or to the "public at large."[43] Instead, the plaintiff must be injured in a "personal and individual way," such that he or she has a "direct stake" in the outcome.[44] Furthermore, "[a]lthough imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is certainly impending."[45] As such, allegations of a "possible *future* injury"[46] are not sufficient to confer standing.

The standing requirement is particularly stringent when "reaching the merits of the dispute would force [the Court] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional."[47] In fact, the Court has "often found

---

content/uploads/2015/02/13-1175-bsac-Professors-Adam-Lamparello-and-Charles-E.-MacLean.pdf.

38 *See* Rubow, *supra* note 9, at 1010.

39 *See* U.S. CONST., art. III, § 2, cl. 2.

40 Rubow, *supra* note 9, at 1010 (quoting Steven L. Winter, *The Metaphor of Standing and the Problem of Self-Governance*, 40 STAN. L. REV. 1371, 1460 (1988)).

41 Rubow, *supra* note 9, at 1010 (quoting ERWIN CHEMERINSKY, FEDERAL JURISDICTION 56 (4th ed. 2003)).

42 *Id.* at 1010 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992)).

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

44 *Id.*

45 Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013) (quoting *Lujan*, 504 U.S. at 565, n.2) (holding that efforts to mitigate injury following a data breach are not cognizable because costs associated with preventing future harm are not sufficiently imminent to confer standing).

46 *Id.* (emphasis added) (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

47 *Id. (*quoting Raines v. Bird, 521 U.S. 811, 819–820 (2003)).

a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs."[48]

The "actual injury" and "imminent harm" requirements affect consumers' ability to recover damages for online data breaches in two ways. First, consumers cannot claim that they have suffered a cognizable injury to their privacy because the moment consumers convey their phone, credit card, and social security numbers to an online service provider, they forfeit their privacy rights. As such, if this information is obtained by third parties, e.g., hackers, consumers will not have standing to sue because, having no expectation of privacy in the unlawfully accessed data, they have not suffered an actual or concrete injury to their privacy rights. This leaves citizens wholly dependent on private companies to implement policies that minimize the risk of online data breaches, and compensate them fully in the event of a breach.

Second, the "imminent harm" requirement largely precludes consumers from suing merchants for the costs incurred when preventing foreseeable—albeit future—damages.[49] In *Clapper v. Amnesty International*, the plaintiffs challenged Section 702 of the Foreign Intelligence Surveillance Act,[50] which authorized the surveillance of individuals who were not "United States persons" and who were located outside of the United States.[51] Several media organizations and civil rights groups filed suit alleging that there was "an objectively reasonable likelihood that their communications with their foreign contacts will be intercepted . . . at some point in the future."[52] The Court rejected this argument and held that the possibility, even likelihood, of future harm was not sufficient to satisfy the "imminent harm" requirement.[53]

The imminency requirement artificially limits the damages consumers can recover when their private information is fraudulently obtained. Admittedly, merchants are required to notify consumers when an online data breach occurs,[54] and if unauthorized charges are

---

[48] *Id.* (citing Laird v. Tatum, 408 U.S. 1, 11–16 (1972) (plaintiffs did not have standing to challenge an Army intelligence-gathering program)).

[49] *See generally* Miles L. Galbraith, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U. L. REV. 1365 (2013).

[50] 50 U.S.C. § 1881(a) (2012).

[51] *Clapper*, 133 S. Ct. at 1140.

[52] *Id.* at 1147.

[53] *Id.* at 1148 (holding that it "is speculative whether the Government will imminently target communications to which respondents are parties").

[54] *See* Caroline C. Cease, Note, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395, 396 (2014) (stating that, "[o]nce the merchant discovers the data breach, it is often obligated under state law to notify its potentially affected customers that their information may have fallen into the wrong hands").

discovered, the merchants will reverse these charges or reimburse the affected consumers.[55] The financial risk to the consumer, however, does not stop there.[56] Hackers may use a consumer's personal identifying information to, among other things, open new credit card accounts and assume the consumer's identity on social media.[57] Thus, consumers may incur substantial cost to prevent such harm, prompting them to monitor their credit report on an ongoing basis. The question then becomes, to what extent will a private company be responsible for the costs associated with mitigation, and for damages that result in the future but are traceable to the initial breach?

At this point, consumers are struggling to recover these costs. In cases where consumers have instituted class action lawsuits for mitigation-related damages, many federal courts have held that these damages are not sufficiently imminent to confer Article III standing.[58] Additionally, the courts have not established parameters governing a merchant's liability for harm that is proximately caused by an online data breach, such as where a hacker opens a new credit card account in a consumer's name and makes purchases under the consumer's name, or where the consumer's credit score is severely damaged.[59]

Furthermore, the law provides no remedy for the non-economic but severely distressful invasion of consumers' privacy rights.[60] None of this is acceptable because it allocates the risk of loss to consumers even though they are in no position to prevent the breach and allows the merchant to escape liability in proximately-caused harms even though it has the power and resources to minimize the risk of these breaches.

For these reasons, the Supreme Court's privacy jurisprudence should adapt to fit the digital era and provide a sufficient remedy for the online data breaches that continue to occur on a widespread scale.[61] The Court should: (1) abandon the first prong of *Katz* and focus exclusively on whether there is a societal expectation of privacy in data voluntarily given to third parties; (2) modify the third-party doctrine to hold that, when a societal expectation of privacy exists, citizens do not forfeit all privacy expectations in information provided to third parties; and (3)

---

55 *See, e.g.*, *id.*; *see also* Natalie Kim, Note, *Three's a Crowd: Towards Contextual Integrity in Third-Party Data Sharing*, 28 HARV. J.L. & TECH. 325 (2014).

56 *See, e.g.*, Cease, *supra* note 54, at 396.

57 *See, e.g.*, Meal, *supra* note 4, at *12; Kori Clanton, Note, *We Are Not Who We Pretend to Be: ODR Alternatives to Online Impersonation Statutes*, 16 CARDOZO J. CONFLICT RESOL. 323, 332 (2014) (discussing online impersonation on social media websites).

58 *See, e.g.*, *Clapper*, 133 S. Ct. 1138; *cf.* Michelle Kisloff & Arthur Kim, *Courts Split on Standing for Consumer Plaintiffs in Data Breach Class Actions*, HOGAN LOVELLS (Dec. 23, 2014), http://www.hldataprotection.com/2014/12/articles/privacy-security-litigation/courts-split-on-standing-for-consumer-plaintiffs-in-data-breach-class-actions.

59 *See, e.g.*, Meal, *supra* note 4, at *3.

60 *See, e.g.*, United States v. Miller, 425 U.S. 435 (1976).

61 *See generally* Laura I. Sorafine & Colin J. Zick, *Protect Your Customers: Solutions to New Privacy and Security Regulations*, 28 No. 5 ACC DOCKET 64 (2010).

relax the "imminent injury" prong to permit recovery for costs associated with preventing future harm, provided that the harm is a reasonably foreseeable result of the breach. This approach will permit recovery for infringements on consumers' privacy, fully compensate consumers for their losses, and provide an incentive for private companies to exercise reasonable care to protect consumers' private information.

Ultimately, we no longer live in a world in which citizens purchase products predominantly with cash, pay their bills with paper checks, or store private information only in their homes. The digital age transcends physical space and finite objects; millions of citizens pay their bills electronically, deposit their paychecks, and purchase books online. They take photographs with and store confidential documents in their cell phones. Thus, private information is exposed—and privacy rights are vulnerable—in a manner that pre-digital era case law never contemplated.[62]

CONCLUSION

The third-party, standing, and reasonable expectation of privacy doctrines make it more difficult for citizens to recover damages directly and proximately caused by online data breaches, and make it less likely that private companies will be incentivized to adopt stringent procedures to protect personal information. In an era of hackers, malware, and inadvertent disclosures of private information, the law should allocate the risk to companies that are in a position to minimize or prevent infringements on consumers' privacy.[63] In the context of online data breaches, abandoning the third-party doctrine, eliminating the "imminent harm" prong of the standing doctrine, and focusing on a societal, not subjective, expectation of privacy, will provide the types of

---

62 To be clear, this argument has nothing to do with the Fourth Amendment, which only applies to state action. *See, e.g.*, Erwin Chemerinsky, *Narrowing the State Action Doctrine*, 35 TRIAL 101 (July 1999) (explaining that the state action doctrine "is the principle that the Constitution's protections of individual liberties . . . apply only to the government. Private conduct generally does not have to comply with the Constitution"). Of course, the National Security Agency's Metadata Collection Program undoubtedly implicates privacy rights, but that is a separate issue. *See, e.g.*, Joshua Peck, Note, *Last Resort: The Threat of Federal Steroid Legislation—Is the Proposed Legislation Constitutional?*, 75 FORDHAM L. REV. 1777 (2006). When dealing with individual privacy rights in non-governmental contexts, tort and contract law can and should provide a remedy. *See, e.g.*, Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 351 (2013). If citizens do not retain privacy rights in information surrendered to third parties, however, they will have no standing and thus no remedy for infringements on privacy violations when hackers obtain their credit card information through a merchant's server. That, in a nutshell, is the problem.

63 *See Chronology of Data Breaches: Security Breaches 2005–Present*, PRIVACY RIGHTS CLEARINGHOUSE (Apr. 20, 2005), http://www.privacyrights.org/data-breach (last updated Dec. 31, 2013).

safeguards that meet the challenges posed by digital era technology.