COURSE CORRECTION—DATA BREACH AS INVASION OF PRIVACY

Jordan Elias*

I. INTRODUCTION**

The news comes by e-mail. Your health insurer has been hacked. You've confided in your doctor, sharing some of your deepest secrets, even that you are HIV-positive. Among the records stolen in the data breach were the doctor's notes. Your social security number, too, was compromised. You are distraught. Months go by and no one tries to steal

*J.D., Stanford Law School, 2003; B.A. magna cum laude, Yale College, 1998. The views and research in this Article are my own.

**Editors' Note: Any deviations from the rules of *The Bluebook: A Uniform System of Citation* (Columbia Law Review Ass'n et al. eds., 20th ed. 2015) are at the author's request for ease of accessibility in electronic format.

your identity or commit any other crime using your personal information. Do you have any legal recourse against the insurer?

Data breach litigation has given rise to new questions, like whether claims may proceed against hacked companies in the absence of fraudulent account activity or actual identity theft affecting those whose information was lost. Courts have recognized a distinction between cases involving actual fraud or identity theft—or, at least, signs of a malicious hack—and cases not involving misuse, as where a thief may have broken into a car and grabbed a laptop without realizing what it contained. Plaintiffs in the first category, who suffered economic loss or were subject to intentional data theft, have been deemed to have standing to sue the hacked company for negligence and other alleged violations. In the second category, plaintiffs whose information was merely exposed, but never exploited, often find themselves out of luck. Highlighting this distinction, the court in *Khan v. Children's National Health System* surveyed existing case law and suggested that plaintiffs can pursue damages if they "provide either (1) actual examples of the use of the fruits of the data breach for identity theft, even if involving other victims; or (2) a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud."[1]

However tidy this "*Khan* dichotomy" may seem, it is also incomplete. The Supreme Court's decision in *Spokeo, Inc. v. Robins* supports applying the common law of privacy to personal data loss.[2] Established privacy principles counsel against tying the fate of claims solely to the criminal intent of hackers or the presence of economic harm from data misuse. Against this legal backdrop, the *Khan* dichotomy of misuse vs. no misuse pays short shrift to the nature of the stolen information and the intangible harm that data breaches can cause.

The news in autumn 2017 that half of all Americans' information had been taken from Equifax left many deeply rattled. As this collective experience shows, the dominant harm from data breaches lies not in low-level fraud but in the loss of private facts themselves and consequent damage of an intangible nature: anxiety, embarrassment, and distress. That these feelings are well founded should be uncontroversial, given the severity and increasing prevalence of identity theft. There is good reason why, even as many people are now resigned to their online searches and

[1] 188 F. Supp. 3d 524, 532 (D. Md. 2016).

[2] 136 S. Ct. 1540 (2016).

purchases being tracked, few would willingly list their medical facts or social security numbers on unencrypted websites.[3]

Several early data breach cases involved the theft of payment card information. Within a few years, economic harm—traditionally incidental and at the periphery of privacy torts—gained a toehold at the core of data breach jurisprudence.[4] A decade into this body of law, courts should embrace invasion of privacy principles, under which the legal rights of victims derive in part from the nature of the information exposed.

Not all types of hacked information carry the same status. Breaches of payment card databases, however large (as in the Target and Home Depot incidents), are of lesser magnitude than certain breaches of medical or governmental systems (as in the Anthem, Premera, and U.S. Office of Personnel Management incidents). A debit or credit card can be canceled or reissued. Private medical information can never be changed and is far more sensitive. Social security numbers—taken, for example, in the massive Equifax breach—can be hoarded and used to steal identities or tax refunds or to inflict other harm years later, after all applicable statutes of limitations have run.

Courts have too often skipped over this hierarchy of personal information in deciding data breach cases. Yet the common law of privacy necessarily looks to the nature of exposed information in determining whether its exposure would offend a reasonable person.

Spokeo recognizes that the common law should guide standing rules in the digital age.[5] Although it was the negligence tort that dominated the early years of data breach litigation,[6] breaches releasing highly sensitive

---

[3] Expectations of privacy surrounding a certain object or piece of information become more reasonable to the extent it is shielded from disclosure instead of being exposed in a public place. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 40–41 (1988) (no reasonable expectation of privacy, for Fourth Amendment purposes, in garbage left on sidewalk in opaque trash bags).

[4] *See* Catherine M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?*, 66 DEPAUL L. REV. 339, 341–42 (2017).

[5] 136 S. Ct. at 1549 ("Because the doctrine of standing derives from the case-or-controversy requirement, and because that requirement in turn is grounded in historical practice, it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."); *see also* City of Ontario v. Quon, 560 U.S. 746, 759 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

[6] *See, e.g.*, *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1170–75 (D. Minn. 2014) (analyzing negligence claims arising from breach of Target's electronic systems

information implicate privacy torts as well. Especially relevant are two aspects of the cause of action for intrusion upon seclusion. First, a defendant may be liable for enabling a privacy invasion even if the defendant did not carry out the invasion.[7] Second, a plaintiff need not have sustained out-of-pocket loss to recover for a privacy invasion because the central damage is the invasion itself and the intangible harm it brings about.[8] Under the common law of privacy, the nature of the stolen information—not just whether it has been misused—should figure prominently in data breach legal analysis.

II. TO MISUSE OR NOT TO MISUSE: THE *KHAN* DICHOTOMY AND ITS LIMITS

A. The Khan *Dichotomy at Work in the U.S. Courts of Appeal*

The *Khan* dichotomy of misuse vs. no misuse can be traced back to a 2007 Seventh Circuit decision, *Pisciotta v. Old National Bancorp*.[9] The court held that data breach victims had standing to sue, reasoning in part that "the scope and manner of access suggests that the intrusion was sophisticated, intentional and malicious."[10] The court disagreed with early district court opinions holding that "plaintiffs whose data has been compromised, but not yet misused, have not suffered an injury-in-fact sufficient to confer Article III standing."[11] But the court affirmed the dismissal of claims under Indiana law where the only alleged harm was plaintiffs' payment for credit monitoring services.[12] Despite the exposure in

---

under the respective laws of each plaintiff's home state); *In re* Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 528–31 (N.D. Ill. 2011) (dismissing negligence claims arising from alleged failure to have prevented "skimming" of debit and credit card numbers).

[7] *See, e.g.*, Carter v. Innisfree Hotel, Inc., 661 So. 2d 1174, 1178 (Ala. 1995); Moore v. New York Elevated R.R. Co., 29 N.E. 997, 998 (N.Y. 1892); *see also infra* Section IV.A.

[8] *See Spokeo*, 136 S. Ct. at 1551 (Thomas, J., concurring) ("In a suit for the violation of a private right, courts historically presumed that the plaintiff suffered a *de facto* injury merely from having his personal, legal rights invaded."); RESTATEMENT (SECOND) OF TORTS § 652H (AM. LAW INST. 1977); *cf.* Andrew Braunstein, *Standing Up for Their Data: Recognizing the True Nature of Injuries in Data Breach Claims to Afford Plaintiffs Article III Standing*, 24 J.L. & POL'Y 93, 126 (2015) (arguing that "data breach plaintiffs [have] standing at the moment their data is lost in a breach"); *see also infra* Section IV.B.

[9] 499 F.3d 629 (7th Cir. 2007).

[10] *Id.* at 632.

[11] *Id.* at 634.

[12] *Id.* at 633, 637, 640.

Pisciotta of social security and payment card numbers, the plaintiffs didn't allege that the breach caused any fraudulent charges or identity theft incidents.[13]

The Seventh Circuit's reluctance to decide *Pisciotta* on standing grounds made no difference to the parties, as the claims were dismissed.[14] The court's reluctance followed the traditional view of standing as calling for a low threshold inquiry that, particularly considering its "abstract and often politicized" character, cannot bear too much weight in resolving cases.[15]

The Third Circuit had no such qualms four years later in *Reilly v. Ceridian Corporation*, affirming a dismissal for lack of standing where plaintiffs alleged that the theft of their social security and checking account numbers caused them to suffer emotional distress and pay for credit monitoring.[16] The court distinguished *Pisciotta* as involving a "sophisticated, intentional and malicious" hack and the Ninth Circuit's intervening decision in *Krottner v. Starbucks Corporation* as involving actual misuse of hacked information.[17] In *Krottner*, the Ninth Circuit held that a plaintiff's alleged "generalized anxiety and stress" from the theft of a Starbucks laptop containing his social security number conferred standing.[18] In another early data breach decision, the First Circuit reinstated claims for negligence and breach of implied contract, concluding that "the thieves were sophisticated; they targeted [the defendant's] data directly; and they

---

[13] *Id.* at 632 ("Significantly, the plaintiffs did not allege any *completed direct* financial loss to their accounts as a result of the breach. Nor did they claim that they or any other member of the putative class *already had been* the victim of identity theft as a result of the breach.").

[14] *Id.* at 632, 640.

[15] 1 WILLIAM B. RUBENSTEIN, NEWBERG ON CLASS ACTIONS § 2.3 (5th ed. 2010); *see also* Attias v. Carefirst, Inc., 865 F.3d 620, 622 (D.C. Cir. 2017) (plaintiffs have a "low bar to establish their standing at the pleading stage."); Cottrell v. Alcon Labs., 874 F.3d 154, 162 (3d Cir. 2017) ("The injury-in-fact requirement is 'very generous' to claimants, demanding only that the claimant 'allege[ ] some specific, "identifiable trifle" of injury.'") (citations omitted); Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992) ("At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we 'presum[e] that general allegations embrace those specific facts that are necessary to support the claim.'").

[16] 664 F.3d 38, 40 (3d Cir. 2011).

[17] *Id.* at 44.

[18] 628 F.3d 1139, 1142 (9th Cir. 2010).

used that data to ring up thousands of charges to customer accounts, including the accounts of many of the plaintiffs."[19]

The Third Circuit, criticizing *Krottner* and *Pisciotta*'s "skimpy rationale" for finding standing, held that the alleged future harm from identity theft was not sufficiently imminent to establish standing in *Reilly*, where no misuse had occurred.[20] Also deemed insufficient were the plaintiffs' credit monitoring payments: "costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the alleged 'increased risk of injury'" the court regarded as speculative.[21] The court didn't address whether the plaintiffs' alleged distress from exposure of their social security numbers might constitute present, intangible harm.

These decisions seemed to augur a circuit split, but their language also pointed toward a means of reconciliation: the *Khan* dichotomy. Thus, the first in a pair of data breach opinions by Seventh Circuit Chief Judge Diane Wood stated that "9,200 of . . . 350,000 [compromised credit] cards were known to have been used fraudulently" and "plaintiffs allege that the hackers *deliberately* targeted Neiman Marcus in order to obtain their credit-card information."[22] The second in the pair similarly emphasized a plaintiff's allegation "that he already ha[d] experienced fraudulent charges."[23] By contrast, the Fourth Circuit's 2017 ruling in *Beck v. McDonald* fell on the "no misuse" side of the *Khan* dichotomy.[24] After a laptop containing their personal information was stolen from a VA hospital, plaintiffs sued for "embarrassment, inconvenience, unfairness, mental distress, and the threat of current and future substantial harm from identity theft and other misuse[.]"[25] The court affirmed the dismissal of claims

---

[19] Anderson v. Hannaford Bros. Co., 659 F.3d 151, 165 (1st Cir. 2011) (alteration in original); *see also In re* Premera Blue Cross Customer Data Sec. Breach Litig., 198 F. Supp. 3d 1183, 1195–1200 (D. Or. 2016) (analyzing claims that asserted a contractual duty to protect data).

[20] *Reilly*, 664 F.3d at 44–46.

[21] *Id.* at 46.

[22] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690, 693 (7th Cir. 2015) (alteration in original) (emphasis added).

[23] Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016).

[24] 848 F.3d 262 (4th Cir. 2017); *see also In re* SuperValu, Inc., 870 F.3d 763, 769–70 (8th Cir. 2017) (affirming dismissal on standing grounds as to plaintiffs who "have not alleged that they have suffered fraudulent charges on their credit or debit cards or that fraudulent accounts have been opened in their names").

[25] *Beck*, 848 F.3d at 267.

under the Privacy Act, as there was "no evidence that the information contained on the stolen laptop ha[d] been accessed or misused or that [the plaintiffs] ha[d] suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information."[26]

It makes some sense, when a data breach compromises payment cards and nothing more sensitive, to ask whether impending harm from account fraud is speculative rather than substantially likely. In *Clapper v. Amnesty International USA*, the Supreme Court held that journalists and human rights workers lacked standing to sue based on the threat of illegal government surveillance of their international communications with suspected terrorists.[27] The Court held that the surveillance threat was not "certainly impending"; in a footnote, the Court also preserved an alternate, "substantial risk" of future harm test for standing.[28] Later revelations from Edward Snowden effectively vindicated the dissenters in *Clapper*—it turned out the NSA was, in fact, unlawfully surveilling international communications with suspected terrorists.[29] *Clapper* consequently demonstrates the hazards of relying on standing doctrine to decide fact-dependent questions. More to the point here, rigid application of the *Khan* dichotomy overlooks "what both the *Clapper* majority and dissent agreed upon: illicit acquisition of personal information," depending on its nature and how it was obtained, may qualify as "cognizable 'injury in fact' in and of itself."[30]

---

[26] *Id.* at 274 (alteration in original). The *Beck* plaintiffs' claims under the Privacy Act, unlike privacy claims at common law, required allegations of "actual damages" to proceed. 5 U.S.C. § 552a(g)(4)(A) (2012). In *FAA v. Cooper*, the Supreme Court held that "actual damages" under the Privacy Act means economic or pecuniary loss—mental or emotional distress does not suffice to merit relief. 566 U.S. 284, 287, 299 (2012).

[27] 568 U.S. 398, 410–14 (2013).

[28] *Id.* at 414 & n.5 (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 153–54 (2010)).

[29] *See* ACLU v. Clapper, 785 F.3d 787, 795–96 (2d Cir. 2015).

[30] Seth F. Kreimer, *"Spooky Action at a Distance": Intangible Injury in Fact in the Information Age*, 18 U. PA. J. CONST. L. 745, 765 (2016). Even when a data breach compromises only payment card information, ensuing intangible harm lends a degree of cohesion to the victims' claims. *See In re* Target Corp. Customer Data Sec. Breach Litig., No. MDL 14-2522 (PAM), 2017 WL 2178306, at *6 (D. Minn. May 17, 2017) ("[A]ll class members in this case suffered the same injury. All class members were the victims of the theft of their personal information and suffered the attendant fear that this information might find its way into the wrong hands on the Internet's black market."); *see also* Smith v. Triad of Alabama, LLC, No. 1:14-CV-324-WKW, 2017 WL 1044692, at *15–16 (M.D. Ala. Mar. 17, 2017) (certifying a class of victims of a hospital data breach and providing for a bifurcated trial with an initial phase dedicated to common questions of

Hence it becomes misplaced to focus only on future harm, and to discount victims' mental distress, when a data breach compromises information like medical records or social security numbers in tandem with birthdates.[31] A fear of identity theft when your social security number has been stolen is well founded, and it is reasonable to feel a sense of outrage when your personal medical facts have been exposed. This information is not only private; it also cannot realistically be changed.[32] Once lost in a data breach, it can never be reclaimed. It can be deployed years later to malevolent ends. Its exposure can cause present, intangible harm that supports standing to sue.

B. Limitations of the Khan *Dichotomy in Data Breach Cases*

Courts shouldn't apply the *Khan* dichotomy of misuse vs. no misuse without also considering case-specific factors unrelated to misuse. The nature of the compromised information looms large in this analysis.[33] Apart

---

duty and breach), *modified in part on reconsideration*, 2017 WL 3816722 (M.D. Ala. Aug. 31, 2017) (modifying the class definition but otherwise denying the defendant hospital's motion to reconsider the class certification order).

[31] *See, e.g.*, *In re* Sci. Applications Int'l Corp. Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 28–29 (D.D.C. 2014) (dismissing, in part, claims for invasion of privacy where stolen data tapes contained medical records and social security numbers).

[32] The Social Security Administration generally will not assign a replacement social security number absent "harassment, abuse, or life endangerment" and will consider doing so only after "you've done all you can to fix the problems resulting from misuse of your Social Security number, and someone is still using your number[.]" Soc. Sec. Admin., *Can I Change My Social Security Number?* (Oct. 21, 2016), *available at* https://faq.ssa.gov/link/portal/34011/34019/Article/3789/Can-I-change-my-Social-Security-number; Soc. Sec. Admin., *Identity Theft and Your Social Security Number*, at 5 (Nov. 2016), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf. Even a "new number probably won't solve all your problems," the Social Security Administration reports. Soc. Sec. Admin., *Identity Theft and Your Social Security Number*, at 6 (Nov. 2016), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf. "This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number," and "credit reporting agencies use the [old] number to identify your credit record." *Id.*; *cf.* Jay Edelson, *Assessing Damages in Privacy Cases*, 26 COMPETITION: J. ANTITRUST & UNFAIR COMP. L. SEC. ST. B. CAL. 161, 165 (2017) (remarking that the "big damage" from data breaches "is the upending of someone's life. . . . If you told someone you can either spend months trying to fix your credit and change all your passwords, or you can have $10 stolen from your wallet, they would say, I'd rather lose the $10. But courts don't recognize that.").

[33] The Office of Management and Budget listed the "Nature of the Data Elements Breached" as the first factor to consider when assessing the severity of a data breach targeting a federal agency. *See* Memorandum for the Heads of Executive Departments and Agencies from Clay

from potential *future* harm, victims of hacking incidents experience intangible *present* harm from the release of confidential information like medical records or social security numbers.

Financial institutions usually reimburse fraudulent payment card charges.[34] The primary threat to consumers from data breaches instead inheres in the psychological effects of knowing that one's unchangeable private facts are now, and maybe forever, in the hands of unknown criminals. The concern naturally arises: why else would the information have been stolen, if not to exploit it? Birthdates and social security numbers can be used together to steal tax refunds and government benefits, assume the victim's identity on social media,[35] prevent victims from obtaining housing and needed medical prescriptions, damage and destroy credit, and

---

Johnson III, Deputy Director of Management, Office of Mgmt. & Budget, M-07-16, at 14–15 (May 22, 2007), *available at* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf (all factors listed were: (1) nature of the data elements breached; (2) number of individuals affected; (3) likelihood the information is accessible and usable; (4) likelihood the breach may lead to harm (both how broad the scope of the harm and how likely it is to occur); and (5) ability of the agency to mitigate the risk of harm); *see also* Daniel Bugni, *Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions*, 52 GONZ. L. REV. 59, 92 (2016/2017) (stating that "[t]he injurious effect of a data breach depends on the nature of the information stolen, the number of records acquired, the length of time before detection, and the sophistication of the hacker."); Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017) (affirming dismissal for lack of standing where "no other personally identifying information—such as [plaintiff's] birth date or Social Security number—is alleged to have been stolen."); *In re* SuperValu, Inc., 870 F.3d 763, 770 (8th Cir. 2017) (affirming, in part, dismissal for lack of standing where "the allegedly stolen [c]ard [i]nformation does not include any personally identifying information, such as social security numbers, birth dates, or driver's license numbers.").

[34] The Truth in Lending Act requires credit card issuers to reimburse all unauthorized charges if the cardholder alerts the issuer before the fraud, or unauthorized charges exceeding $50 if the cardholder does not alert the issuer before the fraud. 15 U.S.C. § 1643 (2012). *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 697 (7th Cir. 2015). In March 2017, Home Depot agreed to pay $25 million to settle claims brought by a class of financial institutions that reimbursed fraudulent charges after hackers breached Home Depot's customer database. *In re* The Home Depot, Inc., Customer Data Sec. Breach Litig., No. 1:14-md-02583-TWT, ECF No. 343 (N.D. Ga. Sept. 22, 2017). Home Depot previously paid more than $140 million to credit card issuers that reimbursed fraudulent charges stemming from the breach. Decl. of Kenneth S. Canfield ¶ 7, *Home Depot*, No. 1:14-md-02583-TWT, ECF No. 327-4 (N.D. Ga. Mar. 8, 2017).

[35] *See* Kori Clanton, *We Are Not Who We Pretend to Be: ODR Alternatives to Online Impersonation Statutes*, 16 CARDOZO J. CONFLICT RESOL. 323, 324 (2014) (discussing online impersonation incidents and statutes).

even commit crimes in victims' names.[36] More than 17 million Americans had their identities stolen in 2014, costing them over $15 billion.[37] In 2016, one out of every 16 Americans experienced identity fraud, an all-time high.[38] The distress from serious data breaches may thus entail feelings of being violated and deprived of control, or of being encroached upon with no solace or escape.[39] Countless Americans experienced these feelings in the fall of 2017, when Equifax announced that hackers had breached its gigantic credit reporting database, stealing social security numbers and other personal facts.

This intangible harm from data breaches resembles "a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts"—invasion of privacy from intrusion upon seclusion.[40] As the Supreme Court observed well before its guidance in *Spokeo*, "[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[41] A legal standard focusing on financial loss obscures the true corrosive dangers of data breach incidents: constriction of the sphere of personal privacy; fear of identity theft; never knowing when, if ever, one's identity might be stolen; and changing one's behavior as a result, for example by checking credit

---

[36] *See generally* IDENTITY THEFT RES. CTR., IDENTITY THEFT: THE AFTERMATH (2016), at 8, *available at* http://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf. Victims have "lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft." U.S. GOV'T ACCOUNTABILITY OFF., GAO-14-34, AGENCY RESPONSES TO BREACHES OF PERSONALLY IDENTIFIABLE INFORMATION NEED TO BE MORE CONSISTENT, at 11 (2013), *available at* http://www.gao.gov/assets/660/659572.pdf.

[37] *See* ERIKA HARRELL, U.S. DEP'T OF JUSTICE, VICTIMS OF IDENTITY THEFT, 2014, at 1, 7 (2015), *available at* https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408. In 2014, the Internal Revenue Service paid an estimated $3.1 billion in fraudulent tax refunds. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-589T, IRS NEEDS TO FURTHER IMPROVE CONTROLS OVER TAXPAYER DATA AND CONTINUE TO COMBAT IDENTITY THEFT REFUND FRAUD, at 1–2 (2016), *available at* http://www.gao.gov/assets/680/676493.pdf.

[38] Al Pascual et al., Javelin Strategy & Research, *2017 Identity Fraud: Securing the Connected Life* (Feb. 1, 2017), *available at* https://www.javelinstrategy.com/coverage-area/2017-identity-fraud.

[39] "Distress," meaning "mental suffering or emotional anguish," is an "injury familiar to the law, customarily proved by showing the nature and circumstances of the wrong and its effect on the plaintiff," including as "evidenced by one's conduct and observed by others." Carey v. Piphus, 435 U.S. 247, 263–64, 264 n.20 (1978).

[40] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).

[41] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

reports obsessively or even delaying educational or other life opportunities.[42]

These are the sorts of adverse consequences that reduce personal liberty and autonomy, creating an imperative for the intrusion upon seclusion tort. The common law protects "certain aspects of the individual and his desired freedom from needless outside interference"—in other words, "a sphere of space that a man may carry with him which is protected from unwarranted outside intrusion[.]"[43] The California Supreme Court has pronounced that:

> [A] measure of personal isolation and personal control over the conditions of its abandonment is of the very essence of personal freedom and dignity, is part of what our culture means by these concepts. A man . . . whose conversations may be overheard at the will of another, whose marital and familial intimacies may be overseen at the will of another, is less of a man, has less human dignity, on that account.[44]

Justice Field believed this as well:

> Of all the rights of the citizen, few are of greater importance or more essential to his peace and happiness than the right of personal security, and that involves, not merely protection of his person from assault, but exemption of his private affairs, books, and papers from the inspection and scrutiny of others. Without the enjoyment of this right, all other rights would lose half their value.[45]

The type of information stolen in a data breach accordingly bears on victims' ability to recover for ensuing intangible harm. With an invasion of privacy claim, "it is both the manner of intrusion as well as the nature of the information acquired that must rise to the level of being highly offensive to

---

[42] *See* IDENTITY THEFT RES. CTR., IDENTITY THEFT: THE AFTERMATH (2016), at 4–6, *available at* http://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf.

[43] Roe v. Ingraham, 403 F. Supp. 931, 936 (S.D.N.Y. 1975), *rev'd on other grounds by* Whalen v. Roe, 429 U.S. 589, 599 (1977) (similarly recognizing "the individual interest in avoiding disclosure of personal matters").

[44] Shulman v. Group W Prods., Inc., 955 P.2d 469, 489 (Cal. 1998) (quoting Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 973–74 (1964)).

[45] *In re* Pac. Ry. Comm'n, 32 F. 241, 250 (N.D. Cal. 1887).

a reasonable person."[46] Thus, "while an individual may have a reasonable expectation of privacy in nude photographs of herself or in her private medical information, she does not have a reasonable expectation of privacy in discussing termination of her employment."[47] Nor is the home address information on a driver's license sensitive enough to receive tort protection.[48] Personal health information contrasts sharply: "The state of a person's gastro-intestinal tract is as much entitled to privacy from unauthorized public or bureaucratic snooping as is that person's bank account, the contents of his library or his membership in the NAACP."[49] Personal health information is rightly "viewed as private and those in possession of it are required to ensure that it is kept secure and used only for proper purposes."[50]

Under a negligence analysis, too, the foreseeability of harm from an entity's ineffective cybersecurity generally corresponds to the sensitivity of the personal information housed in its systems. Under the same analysis, a breached entity may be able to show that it appropriately calibrated its actions to the risks.

Finally, taking into account the nature of the data lost in a hacking incident aids in interpreting the traceability as well as the injury-in-fact prong of standing analysis.[51] If the reported misuse could have been committed with the stolen information, traceability is more likely to be

---

[46] Houck v. Corrections Corp. of Am., No. 15-9586-JAR-TJJ, 2017 WL 347503, at *5 (D. Kan. Jan. 24, 2017).

[47] Kennedy v. City of Braham, 67 F. Supp. 3d 1020, 1035 (D. Minn. 2014).

[48] *See, e.g.*, Rollins v. City of Albert Lea, 79 F. Supp. 3d 946, 961 (D. Minn. 2014) (finding that the plaintiff's "home address, color photograph, date of birth, eye color, height, weight, [and] driver identification number" were "not particularly sensitive in nature, and individuals routinely turn over such information when they show their driver's license").

[49] Bd. of Med. Quality Assurance v. Gherardini, 156 Cal. Rptr. 55, 61 (Ct. App. 1979); *see also* Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) (holding that "[t]he reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."); McKay v. Geadah, 50 Pa. D. & C.3d 435, 446 (Ct. Com. Pl. 1988) (finding that the improper disclosure of private medical facts "could be highly offensive to a reasonable person of ordinary sensibilities").

[50] *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 641 (3d Cir. 2017) (Shwartz, J., concurring in the judgment).

[51] *See* Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 103 (1998) (requiring "a fairly traceable connection between the plaintiff's injury and the complained-of conduct of the defendant"); Bennett v. Spear, 520 U.S. 154, 171 (1997) (referring to the "relatively modest" burden of pleading traceability).

satisfied.[52] But if there is a mismatch between the reported misuse and the stolen information—for instance, identity theft when no social security numbers were taken—there is reason to doubt that the misuse resulted from the data breach in question.

III. *SPOKEO* AND THE INVASION OF PRIVACY TORT

While not a data breach case, *Spokeo* endorses turning to common law analogues to determine a plaintiff's standing to sue for a statutory violation.[53] *Spokeo* concerned claims under the Fair Credit Reporting Act (FCRA) based on a website providing inaccurate information about the plaintiff, misinformation he alleged impaired his ability to get hired.[54] The Supreme Court held that whether an asserted injury meets the Article III standing requirements depends on whether the injury is '"real', and not 'abstract'"—which raises the question of what injuries are "real" enough to be actionable.[55] The Court gave only a partial answer.[56] It advised that "intangible injuries can nevertheless be concrete" and that "both history and the judgment of Congress play important roles" when it comes to evaluating whether an intangible harm is sufficiently concrete to give rise to standing.[57] By "history" the Court had in mind the history of English and American common law decisions: "[I]t is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[58]

Reasonable jurists can interpret this open-ended guidance differently in the data breach setting. In *In re Horizon Healthcare Services Inc. Data Breach Litigation*, the Third Circuit in 2017 overturned a dismissal for lack of standing to pursue FCRA claims arising from an insurer data breach that may have compromised, among other information, social security numbers

---

[52] *See, e.g.*, Resnick v. AvMed, Inc., 693 F.3d 1317, 1327 (11th Cir. 2012) ("Plaintiffs allege a nexus between the two events that includes more than a coincidence of time and sequence: they allege that the sensitive information on the stolen laptop was the same sensitive information used to steal Plaintiffs' identity.").

[53] 136 S. Ct. 1540, 1544, 1547 (2016).

[54] *Id.* at 1544; *id.* at 1554, 1556 (Ginsburg, J., dissenting).

[55] *Id.* at 1548 (opinion of the Court).

[56] *See id.* at 1548–50.

[57] *Id.* at 1549.

[58] *Id.*

and personal medical histories showing "test and lab results[.]"[59] The majority concluded that Congress, in enacting FCRA, enshrined aspects of privacy common law by "establish[ing] that the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself—whether or not the disclosure of that information increased the risk of identity theft or some other future harm."[60] The plaintiffs had standing, the majority reasoned, because they alleged just the sort of unauthorized dissemination Congress prohibited.[61] Judge Shwartz, concurring in the judgment, would have found standing purely on historical grounds:

> The common law has historically recognized torts based upon invasions of privacy and permitted such claims to proceed even in the absence of proof of actual damages. . . . While Plaintiffs do not allege that the laptop thieves looked at or used their PII and PHI, Plaintiffs lost their privacy once it got into the hands of those not intended to have it.[62]

Horizon Healthcare should be influential, not merely because of the opinions' diverging applications of *Spokeo* but because both opinions held that present, not future, harm from loss of privacy occasioned by a data breach conferred standing.[63] For this reason, *Horizon Healthcare* supplies a counterweight to the *Khan* dichotomy, particularly when hackers have breached a computer network to extract highly sensitive data. Then privacy principles come to the fore.

With the progress of "[m]odern life" and advances in technology, the law affords protection to "the individual who desires seclusion and freedom from intrusion into his private life[.]"[64] Data breaches implicate the first branch of the invasion of privacy tort—intrusion upon seclusion, which

---

[59] 846 F.3d 625, 629 (3d Cir. 2017). A plaintiff's income tax refund was stolen after a fraudulent return was filed in his and his wife's names. *Id.* at 630.

[60] *Id.* at 639. One of FCRA's express purposes is "to require that consumer reporting agencies adopt reasonable procedures . . . with regard to the confidentiality, accuracy, relevancy, and proper utilization of [consumers'] information . . . ." 15 U.S.C. § 1681(b) (2012).

[61] *Horizon Healthcare*, 846 F.3d at 640.

[62] *Id.* at 642 (Shwartz, J., concurring in the judgment).

[63] *Spokeo*, 136 S. Ct. at 1549; *Horizon Healthcare*, 846 F.3d at 639 & n.19; *id.* at 642 (Shwartz, J., concurring in the judgment).

[64] Peay v. Curtis Publ'g Co., 78 F. Supp. 305, 309 (D.D.C. 1948).

does not require any publicity, publication, or appropriation.[65] Instead, "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[66] A showing that the defendant acted recklessly may satisfy the element of intent.[67] Whether the alleged invasion is "highly offensive to a reasonable person" ordinarily presents a fact question,[68] and there are a wide and evolving variety of avenues by which an individual's privacy may be invaded.[69] The Restatement specifically recognizes that the "compilation of elaborate written or computerized dossiers" containing personal data may warrant increasing application of the invasion of privacy tort.[70] That an unexpected technique, like hacking, is used to interfere with privacy further supports the cause of action: "If the means used is abnormal in character for gaining access to private information, then the intrusion is likely to be actionable regardless of the purpose."[71] And the tort sweeps beyond physical invasions: "Although intrusion upon seclusion clearly encompasses an intrusion upon a physical space held in seclusion by a person, the element of seclusion also

---

[65] According to the influential Restatement, there are four customary branches of the invasion of privacy tort: (1) Intrusion Upon Seclusion (§ 652B); (2) Appropriation of Name or Likeness (§ 652C); (3) Publicity Given to Private Life (§ 652D); and (4) Publicity Placing Person in False Light (§ 652E). RESTATEMENT (SECOND) OF TORTS §§ 652B–E (AM. LAW INST. 1977).

[66] *Id.* § 652B.

[67] *See, e.g.*, Filotei v. Booth Broad. Co., No. 43454, 1981 WL 4676, at *3 (Ohio Ct. App. Dec. 10, 1981) (holding that "in an action for invasion of privacy, the plaintiff need show either intentional or reckless conduct that resulted in an invasion of plaintiff's privacy."); Smith v. Bob Smith Chevrolet, Inc., 275 F. Supp. 2d 808, 822 (W.D. Ky. 2003) (denying summary judgment because evidence could show that a defendant alleged to have intruded upon the plaintiff's seclusion, by accessing his credit report without his permission, "acted with such reckless disregard for [his] privacy as to amount to an intentional tort."); *see also In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 293–94 (3d Cir. 2016) (holding the intent element satisfied, for pleading purposes, by reference to the plaintiffs' lack of consent to the alleged intrusion), *cert. denied sub nom.* C.A.F. v. Viacom Inc., 137 S. Ct. 624 (2017).

[68] Reid v. LVNV Funding, LLC, No. 2:14CV471DAK, 2016 WL 247571, at *8 (D. Utah Jan. 20, 2016); Rollins v. City of Albert Lea, 79 F. Supp. 3d 946, 960 (D. Minn. 2014); *see also* Walker v. Jackson, 952 F. Supp. 2d 343, 353–54 (D. Mass. 2013); Harms v. Miami Daily News, Inc., 127 So. 2d 715, 718 (Fla. Dist. Ct. App. 1961); Strickler v. Nat'l Broad. Co., 167 F. Supp. 68, 71 (S.D. Cal. 1958).

[69] *See* RESTATEMENT (SECOND) OF TORTS §§ 652A, 652B (AM. LAW INST. 1977).

[70] *Id.* § 652 cmt. c.

[71] PROSSER & KEETON ON THE LAW OF TORTS § 117, at 856 (5th ed. 1984).

encompasses intrusions into a person's private concerns based upon a reasonable expectation of privacy in that area."[72] Liability therefore may be premised on "some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, [or] examining his private bank account[.]"[73] A pair of Depression-era opinions, for example, enjoined unauthorized scrutiny of bank accounts.[74] Other scenarios include peering into the windows of another person's home, searching someone else's shopping bag in a store, and eavesdropping by wiretapping.[75] "In short, 'the core of this tort is the offensive prying into the private domain of another.'"[76]

The indefinite exposure of personal matters from data breaches greatly distresses reasonable people.[77] Nearly all states and territories, recognizing the value of personal information and the social interest in keeping it secure, have enacted laws requiring a hacked company to promptly disclose the incident.[78] Even with many Americans now resigned to being tracked

---

[72] Doe v. High-Tech Inst., Inc., 972 P.2d 1060, 1068 (Colo. App. 1998).

[73] RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (AM. LAW INST. 1977).

[74] Zimmermann v. Wilson, 81 F.2d 847, 847, 849 (3d Cir. 1936); Brex v. Smith, 146 A. 34, 37 (N.J. Ch. 1929); *see also* S.E.C. v. Jerry T. O'Brien, Inc., 467 U.S. 735, 745–46 (1984) (discussing the Right to Financial Privacy Act, 12 U.S.C. § 3401 *et seq.*).

[75] PROSSER & KEETON ON THE LAW OF TORTS § 117, at 854–56 (5th ed. 1984).

[76] Angelo v. Moriarty, No. 15 C 8065, 2016 WL 640525, at *4 (N.D. Ill. Feb. 18, 2016) (quoting Lovgren v. Citizens First Nat'l Bank of Princeton, 534 N.E.2d 987, 989 (Ill. 1989)).

[77] *See, e.g.*, Adam Levin, *The Data Breach Factor So Many Companies Forget: Emotion*, ABCNEWS (Mar. 29, 2014), *available at* http://abcnews.go.com/Business/data-breach-factor-companies-forget-emotion/story?id=23101613.

[78] ALASKA STAT. § 45.48.010 (2016); ARIZ. REV. STAT. ANN. § 18-545 (2015 & Supp. 2016); ARK. CODE ANN. § 4-110-101 (2011); CAL. CIV. CODE §§ 1798.29, 1798.82 (West 2009 & Supp. 2017); COLO. REV. STAT. ANN. § 6-1-716 (West 2002 & Supp. 2016); CONN. GEN. STAT. ANN. § 36A-701b (West 2011 & Supp. 2017); DEL. CODE ANN. tit. 6, § 12B-102 (2013); D.C. CODE § 28-3852 (2001 & Supp. 2017); FLA. STAT. ANN. § 501.171 (West 2014); GA. CODE ANN. § 10-1-912 (West 2003 & Supp. 2016); 9 GUAM CODE ANN. § 48.30 (2017), *available at* http://www.guamcourts.org/CompilerofLaws/GCA/09gca/9gc048.pdf; HAW. REV. STAT. ANN. § 487N-2 (LexisNexis 2012); IDAHO CODE § 28-51-105 (2017 & Supp. 2017); 815 ILL. COMP. STAT. ANN. 530/10 (West 2015 & Supp. 2017); IND. CODE ANN. § 24-4.9-3-1 (West 2007); IOWA CODE ANN. § 715C.2 (West 2010 & Supp. 2017); KAN. STAT. ANN. § 50-7a02 (1997 & Supp. 2016); KY. REV. STAT. ANN. § 365.732 (LexisNexis Supp. 2016); LA. STAT. ANN. § 51.3074 (2009); ME. REV. STAT. ANN. tit. 10, § 1348 (2002 & Supp. 2016); MD. CODE ANN., COM. LAW § 14-3504 (LexisNexis 2013); MASS. ANN. LAWS ch. 93H, § 3 (LexisNexis 2012); MICH. COMP. LAWS SERV. §§ 445.63, 445.72 (LexisNexis 2013); MINN. STAT. ANN. § 325E.61 (West 2012); MISS. CODE ANN. § 75-24-29 (Supp. 2016); MO. ANN. STAT. § 407.1500 (West 1998); MONT. CODE ANN. §§ 30-14-1704, 33-19-321 (2015); NEB. REV. STAT. ANN. § 87-803 (LexisNexis 2012

and bombarded with targeted ads, it is far more troubling to know that criminals could steal your identity, even blackmail you, with the information they've stolen. The core harms from serious data breaches are the same harms that characterize the intrusion upon seclusion tort: anxiety and anguish from a loss of personal privacy.

IV. THE INVASION OF PRIVACY TORT SHOULD INFORM THE ANALYSIS IN CASES INVOLVING SERIOUS DATA BREACH INCIDENTS.

In data breach cases involving at least the exposure of social security numbers, invasion of privacy claims may best capture the essential violation and harm. In *Rowe v. UniCare Life & Health Insurance Company*, a Chicago district court upheld an invasion of privacy claim after an insurer allowed the plaintiff's protected health information to be temporarily available to the public online, even though the plaintiff didn't allege anyone had viewed his information.[79] The court explained that "in the case of an invasion of privacy action, proof of actual harm need not be of pecuniary loss and actual harm may include damages for emotional distress."[80]

UniCare serves as an instructive precedent for data breach cases on the severe end of the spectrum. Yahoo! Inc. announced in late 2016 that it had suffered two enormous data breaches compromising information associated with hundreds of millions of Yahoo e-mail accounts.[81] The company said

& Supp. 2016); NEV. REV. STAT. ANN. § 603A.220 (West 2016); N.H. REV. STAT. ANN. § 359-C:20 (LexisNexis 2008); N.J. STAT. ANN. § 56:8-163 (West 2012); N.M. STAT. ANN. § 57-12C-6 (LexisNexis 2017); N.Y. GEN. BUS. LAW § 899-aa (LexisNexis 1999 & Supp. 2017); N.C. GEN. STAT. § 75-65 (2015); N.D. CENT. CODE § 51-30-02 (2007 & Supp. 2017); OHIO REV. CODE ANN. § 1349.19 (LexisNexis 2012); OKLA. STAT. ANN. tit. 24, § 24-163 (West 2012 & Supp. 2017); OR. REV. STAT. § 646A.604 (2015); 73 PA. STAT. AND CONS. STAT. ANN. § 2303 (West 2003); P.R. LAWS ANN. tit. 10, § 4052 (2012); 11 R.I. GEN. LAWS § 11-49.3-4 (Supp. 2016); S.C. CODE ANN. § 39-1-90 (2016); TENN. CODE ANN. § 47-18-2107 (2014 & Supp. 2016); TEX. BUS. & COM. CODE ANN. § 521.053 (West 2009); UTAH CODE ANN. § 13-44-202 (LexisNexis 2015); VT. STAT. ANN. tit. 9, § 2435 (2014); VA. CODE ANN. §§ 18.2-186.6, 32.1-127.1:05 (2014); V.I. CODE ANN. tit. 14, § 2208 2012; WASH. REV. CODE ANN. §§ 19.255.010, 42.56.590 (West 2013 & Supp. 2017); W. VA. CODE §§ 46A-2A-101–102; (LexisNexis 2015); WIS. STAT. ANN. § 134.98 (West 2016); WYO. STAT. ANN. §§ 40-12-501–502 (2017).

[79] No. 09 C 2286, 2010 WL 86391, at *1, *9 (N.D. Ill. Jan. 5, 2010).

[80] *Id.* at *9 (internal quotation marks omitted) (citing RESTATEMENT (SECOND) OF TORTS § 652H cmts. b & c (AM. LAW INST. 1977)).

[81] Vindu Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), *available at* https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?mcubz=0.

that among the information possibly hacked were passwords and "encrypted or unencrypted security questions and answers."[82] Class actions arising from these incidents are pending in federal court in San Jose, near Yahoo's headquarters.[83] With existing case law prioritizing out-of-pocket loss, plaintiffs invoked a litany of fraudulent charges to justify their claims.[84] Yet that basis for relief seems misaligned with the invasion. If criminals could now log into individual Yahoo e-mail accounts, they would have access to the equivalent of a huge cache of personal letters. And under common law, "[j]ust as private individuals have a right to expect that their telephonic communications will not be monitored, they also have a reasonable expectation that their personal mail will not be opened and read by unauthorized persons."[85] After a similar hack, on a comparatively smaller scale, of Sony Pictures Entertainment—which agents of North Korea allegedly perpetrated to retaliate for the movie *The Interview*—screenwriter Delia Ephron wrote, only half-jokingly, that "the thing that freaked me out most . . . was not the theft of my Social Security number but the capture and

---

[82] Press Release, Yahoo! Inc., An Important Message to Yahoo Users on Security (Sept. 22, 2016), *available at* http://www.businesswire.com/news/home/20160922006198/en/; Bob Lord, *Important Security Information for Yahoo Users* (Dec. 14, 2016), *available at* https://yahoo.tumblr.com/post/154479236569/important-security-information-for-yahoo-users. On February 28, 2017, a federal grand jury charged two Russian intelligence officers with perpetrating the mammoth Yahoo hack. *See* Indictment, United States v. Dokuchaev, No. 17-103 (N.D. Cal.), *available at* https://www.justice.gov/opa/press-release/file/948201/download. On October 3, 2017, Yahoo revealed that the attack compromised each of the approximately 3 billion Yahoo e-mail accounts then in existence. Press Release, Yahoo! Inc., Yahoo Provides Notice to Additional Users Affected by Previously Disclosed 2013 Data Theft (Oct. 3, 2017), *available at* https://www.sec.gov/Archives/edgar/data/732712/000073271217000003/a2017_10x3xoathxexhibitx991.htm.

[83] *See In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, at *1–2 (N.D. Cal. Aug. 30, 2017).

[84] *See id.* at *4–5.

[85] Vernars v. Young, 539 F.2d 966, 969 (3d Cir. 1976). In a September 2016 letter to the Yahoo CEO, six U.S. Senators wrote that the stolen data can be used "not only to access Yahoo customer accounts, but also potentially to gain access to any other account or service that users access with similar login or personal information, including bank information and social media profiles." Letter from Richard Blumenthal et al., Senator, U.S. Senate, to Marissa Mayer, CEO, Yahoo! Inc. (Sept. 27, 2016), *available at* https://www.leahy.senate.gov/imo/media/doc/9-27-16%20Yahoo%20Breach%20Letter.pdf.

exposure of personal email. . . . Exposure of my emails would reveal not only deep fears and worries, but also my shallow personality."[86]

A. A Company That Enables a Data Breach Can Be Liable for Invasion of Privacy.

Data breach defendants often maintain that it is they who were victimized by third-party criminal hacking.[87] That may be; but just as a defendant can be liable for negligence consisting of inaction, so can a defendant be liable for recklessly leaving the electronic door open to hackers.[88] The D.C. Circuit recognized this possibility in 2017, reinstating a data breach lawsuit even though "the thief would be the most immediate cause of plaintiffs' injuries" and the defendant's "failure to secure its customers' data would be one step removed in the causal chain."[89] Two "peeping Tom" cases decided a century apart demonstrate that entities can be held to account for enabling privacy invasions carried out by third-party individuals.[90]

First, around the time Warren and Brandeis published their "Right to Privacy" article,[91] New York's high court decided *Moore v. New York*

---

[86] Delia Ephron, Opinion, *It's a Whole New Paranoid World*, N.Y. TIMES, Mar. 22, 2015, at SR3, *available at* https://www.nytimes.com/2015/03/22/opinion/sunday/its-a-whole-new-paranoid-world.html?_r=0. Sony defended, then settled, class claims brought by victims of the November 2014 cyberattack. *See* Corona v. Sony Pictures Entm't, Inc., No. CV 14-09600-RGK (Ex), 2015 WL 12655592, at *1 (C.D. Cal. Nov. 24, 2015), *and* 2015 WL 3916744, at *1 (C.D. Cal. June 15, 2015).

[87] *See, e.g.*, Consolidated Brief of Defendant-Appellee Nationwide Mutual Ins. Co. at 3, Galaria v. Nationwide Mut. Ins. Co., Nos. 15-3386, 15-3387, 2015 WL 6460120, at *3 (3d Cir. Oct. 22, 2015) (stating that the defendant company "was the victim of a criminal attack on a portion of its computer network."); Brief of Appellees/Cross-Appellants at 1, Anderson v. Hannaford Bros. Co., Nos. 10-2384, 10-2450, 2011 WL 1836177, at *1 (1st Cir. Apr. 25, 2011) (stating that the defendant company "fell victim to a criminal data breach.").

[88] *See* Samson v. Saginaw Prof'l Bldg., Inc., 224 N.W.2d 843, 848 (Mich. 1975) (defining "the basic element of all negligence" as "failure to act as a reasonable man would."); JUDICIAL COUNCIL OF CALIFORNIA CIVIL JURY INSTRUCTIONS, CACI No. 401 (2017) ("A person is negligent if he or she . . . fails to do something that a reasonable careful person would do in the same situation."); *cf. supra* note 67.

[89] Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017).

[90] *See* Moore v. N.Y. Elevated R.R. Co., 130 N.Y. 523, 523–24 (1892); Carter v. Innisfree Hotel, Inc., 661 So. 2d 1174 (Ala. 1995).

[91] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

Elevated Railroad Company.[92] The railroad had built an elevated platform next to a Manhattan apartment building, and railroad passengers and workers on the platform could look in on people in apartments.[93] The court held that the railroad could be liable for the intrusion on seclusion: Where "the [railroad] furnished the means and opportunity for the [passengers and workers] to invade the privacy of these rooms," the court could detect "[n]o reason . . . why the [railroad] should not be responsible for the consequences of the loss of privacy thus occasioned[.]"[94]

Second, in the salacious case of *Carter v. Innisfree Hotel, Inc.*, a married couple who had checked into a hotel, planning to attend a concert that evening, heard knocking and scratching sounds behind the bathroom mirror while they were eating fast food in their room.[95] Thinking nothing of it, they then spent several hours having sex and lounging around naked—only to discover peep holes in the bathroom mirror![96] Husband and wife testified that the incident caused them to suffer insomnia, nervousness, and marital strains.[97] The trial court entered summary judgment for the hotel, but the Alabama Supreme Court reversed in part, holding that the hotel could be liable for intruding on the couple's privacy even if "a third party" unaffiliated with the hotel looked in on them.[98]

As the hotel didn't close up the peep holes in its mirrors, hacked companies often haven't plugged the holes in their cybersecurity. Most electronic breaches can be prevented through prudent countermeasures, such as two-factor security authentication,[99] and the rash of prominent

---

[92] 130 N.Y. 523 (1892).

[93] *Id.* at 526–27.

[94] *Id.* at 528.

[95] 661 So. 2d at 1177.

[96] *Id.*

[97] *Id.* at 1177–78.

[98] *Id.* at 1178–79.

[99] *See, e.g.*, Press Release, Online Trust Alliance, OTA Determines Over 90% of Data Breaches in 2014 Could Have Been Prevented (Jan. 21, 2015), *available at* https://otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented; H.R. COMM. ON OVERSIGHT & GOV'T REFORM, 114TH CONG., THE OPM DATA BREACH: HOW THE GOVERNMENT JEOPARDIZED OUR NATIONAL SECURITY FOR MORE THAN A GENERATION, at viii (2016), *available at* https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

breaches has given notice of the threat.[100] The hacked company, therefore, may be seen as having recklessly provided "the means and opportunity" (as in the New York railroad case) for hackers to gain intimate details of people's lives.[101] In that scenario, the company can't shield itself behind the hackers' criminal acts because a defendant may be liable for enabling an invasion of privacy completed by a third party.

B. A Plaintiff Need Not Sustain Economic Loss to Recover for a Privacy Invasion from a Data Breach.

Damages are typically for the privacy violation alone; a plaintiff whose privacy was invaded need not establish a specific loss. The Supreme Court noted that, "Traditionally, the common law has provided such victims with a claim for 'general' damages, which for privacy and defamation torts are presumed damages: a monetary award calculated without reference to specific harm."[102]

A plaintiff whose seclusion has been invaded "may also recover damages for emotional distress or personal humiliation that he proves to have been actually suffered by him, if it is of a kind that normally results from such an invasion and it is normal and reasonable in its extent."[103] Though "mental and subjective," these kinds of injury "may cause suffering much more acute than that caused by a bodily injury."[104]

Ever since the invasion of privacy tort emerged, the dominant harms it has redressed have been humiliation and personal offense, without need for physical or economic damage. The first American case to recognize a cause of action for invasion of privacy, in 1881, involved "damages . . . from shame and mortification" experienced by a woman whose childbirth was

---

[100] *See* IDENTITY THEFT RES. CTR., ITRC BREACH STATISTICS 2005-2016 (2016), *available at* http://www.idtheftcenter.org/images/breach/Overview2005to2016Finalv2.pdf (detailing 471 data breaches in 2012, 614 in 2013, 783 in 2014, and 780 in 2015).

[101] Moore v. N.Y. Elevated R.R. Co., 130 N.Y. 523, 528 (1892).

[102] Doe v. Chao, 540 U.S. 614, 621, 621 n.3 (2004); *see also, e.g.*, Munden v. Harris, 134 S.W. 1076, 1077 (Mo. Ct. App. 1911) (rejecting the defendant's argument that "the law does not afford redress for an invasion by one person of another's privacy, unless it is accompanied by some injury to his property or interference therewith"); Pavesich v. New Eng. Life Ins. Co., 50 S.E. 68, 73 (Ga. 1905) (holding that "a violation of the right of privacy is a direct invasion of a legal right of the individual. It is a tort, and it is not necessary that special damages should have accrued from its violation in order to entitle the aggrieved party to recover.").

[103] RESTATEMENT (SECOND) OF TORTS § 652H (AM. LAW INST. 1977).

[104] Fairfield v. Am. Photocopy Equip. Co., 291 P.2d 194, 197 (Cal. Ct. App. 1955).

invaded by her doctor bringing along a young unmarried man—identified only as "Scattergood"—who was neither a doctor nor a nurse but who held her hand during contractions.[105] And a case often cited for the principle that even in public, some things remain private, also shows that the primary harm from invasion of privacy is intangible.[106] The plaintiff in *Daily Times Democrat v. Graham* sustained no monetary loss but recovered damages for being embarrassed, self-conscious, and upset after the local paper printed a photograph of her with her dress unexpectedly blown up in a "Fun House" at the county fair.[107] Other plaintiffs could recover for distress when they found out that cameras or listening devices had been secretly installed in places they frequented, regardless whether the devices were used.[108]

Likewise, in serious data breach cases, the simple exposure of personal information may cause present, intangible harm in the form of mental or emotional distress, whether or not that information has been—or ever will be—misused.

V. CONCLUSION

Hacking of sensitive personal information remains grossly offensive. To optimize defensive measures, public policy favors generally allocating the burden of ensuring security to the entity housing the information. Courts faced with the circumstances of particular data breaches should draw upon the body of privacy common law in rendering decisions. Relevant is not just whether there has been misuse but also what information was stolen. Under traditional privacy law concepts, the more confidential that information is, the stronger the claim to recovery will be.

---

[105] De May v. Roberts, 9 N.W. 146, 146, 149 (Mich. 1881).

[106] Daily Times Democrat v. Graham, 162 So. 2d 474 (Ala. 1964).

[107] *Id.* at 476.

[108] *See* Harkey v. Abate, 346 N.W.2d 74, 76 (Mich. Ct. App. 1984) (installation of hidden cameras in a skating rink bathroom was an invasion of privacy, without regard to whether they were used); Hamberger v. Eastman, 206 A.2d 239, 242 (N.H. 1964) (secret installation of a listening device in another's home was an invasion of privacy, without regard to whether it was used).