University of Georgia Law

Journal of Intellectual Property Law

Volume 25 | Issue 2 Article 3

October 2018

A Duty to Safeguard: Data Breach Litigation Through a Quasi-Bailment Lens

Miles Christian Skedvold
University of Georgia School of Law

A DUTY TO SAFEGUARD: DATA BREACH LITIGATION THROUGH A QUASI-BAILMENT LENS

Miles Christian Skedsvold[*]

[*] J.D. Candidate, 2019. Special thanks to Professor David Shipley for his feedback and advice in sponsoring this note.

I. INTRODUCTION

This Note was not originally about Equifax. I decided to write a Note about Data Breach Litigation during my 1L summer internship, after working on the early stages of a putative class action lawsuit against a healthcare provider. The breach involved compromising the personally identifiable information (PII)—including sensitive medical information—of as many as 531,000 people. At the time, I thought that was a lot.

The project ended up occupying a fair amount of my time that summer, and by the time classes started back I thought I had something of a pet theory for stating a common law claim for negligent data security. This Note will make the case for that theory.

Then Equifax. In early September, news broke that Equifax had been the victim of one of the largest data breaches ever recorded.[1] The breach, Equifax told us, compromised the personally identifiable information of as many as 143 million Americans—nearly half the adult population of the United States.[2] Perhaps most striking was CNN's report that

[u]nlike other data breaches, not all of the people affected by the Equifax breach may be aware that they're customers of the company. Equifax gets its data from credit card companies, banks, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies, as well as by purchasing public records.[3]

It wasn't long before I would tell a classmate, a professor, or a friend about my Note topic, and they would reply, "Oh cool, so you're writing about Equifax?" And so it was—my Note was swept up in the breach. Fine. I guess I'm writing about Equifax.

But, in reality, there is more than that at stake here. What I fear will escape notice is that, depending on who you ask, Equifax isn't even the largest recorded data breach,[4] and it certainly wasn't the only one this year. Said another way, this was *not* a one-off event. Years before the Equifax breach, data from the U.S. Department of Health and Human Services noted 1,059 breaches impacting

[1] Sarah Ashely O'Brien, *Giant Equifax data breach: 143 million people could be affected*, (Sept. 8, 2017, 9:23 AM), http://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html.

[2] *Id.*

[3] *Id.*

[4] Mark Fahey, *Yahoo data breach is among the biggest in history* (Sept. 22, 2016, 3:09 PM), https://www.cnbc.com/2016/09/22/yahoo-data-breach-is-among-the-biggest-in-history.html.

close to 32 million individuals.[5] In 2017 alone, Yahoo, Uber, Verizon, and NetProspex all suffered breaches affecting no less than 14 million people—each.[6]

Even before news of the Equifax Breach broke, data security concerns were becoming more common and more pressing. "In the course of our everyday activities, we routinely reveal our names, addresses, and social security numbers as well as our financial decisions, health problems, tastes, habits, political and religious affiliations, sexual orientation, hobbies, and love affairs."[7] Some such transactions are unavoidable, like healthcare, insurance, employment and taxation, and even benefits and entitlements. The frightening reality is that once the information is conveyed, one loses the ability to ensure its security.

Certainly, steps can be taken to protect oneself against identity theft and related harm—but no system is foolproof. Moreover, even to the extent such harm can be remedied, it is not difficult to imagine contexts in which a credit freeze or similar circumstances can cause meaningful harm by hobbling a person's ability to make large scale and important purchases. The more immediate impact, however, is seen in the estimated $4.1 billion consumers would end up paying to freeze their credit.[8]

The other side of the data-breach coin is that commercial entities collecting and storing large quantities of PII face a constant threat of criminal hacking to steal and sell customer PII on the black market.[9] Estimates placed Equifax's losses from the breach between $200 and $300 million by Christmas 2017.[10] Moreover, it is virtually impossible to monetarily gauge what is, without a doubt, an unprecedented loss of consumer confidence in corporate information storage.[11]

Where there is a loss, there is a lawsuit. On September 11th, 2017, less than a week after the breach was announced, Reuters reported that more than thirty lawsuits had already been filed.[12] It appears that dozens more were filed in

[5] Eduard Goodman, *The Equifax Data Breach And Its Impact On Businesses* (Sept. 14, 2017, 2:36PM),https://www.law360.com/articles/963870/the-equifax-data-breach-and-its-impact-on-businesses.

[6] Robin Kurzer, *Equifax and beyond: How data breaches shaped 2017* (Dec, 21, 2017, 10:30 AM), https://marketingland.com/equifax-beyond-data-breaches-shaped-2017-230569.

[7] Vera Bergelson, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 381 (2003).

[8] Kurzer, *supra* note 6.

[9] *See generally* Monique C.M. Leahy, *Litigation of Data Breach*, 140 Am. Jur. Trials 327 § 1, Westlaw (database updated Feb. 2018).

[10] Kurzer, *supra* note 6.

[11] *Id.*

[12] Reuters Staff, *Lawsuits against Equifax pile up after massive data breach* (Sept. 11, 2017, 2:52 PM),https://www.reuters.com/article/us-equifax-cyber-lawsuits/lawsuits-against-equifax-pile-up-after-massive-data-breach-idUSKCN1BM2E3.

subsequent weeks,[13] but exact numbers are difficult to estimate amid consolidations, venue changes, voluntary dismissals, and suits against Equifax unrelated to the breach. Most of these are still in the early stages as this Note is being revised in early January 2018. These include individuals, financial institutions,[14] and even the City of San Francisco.[15]

While most states have statutes that require consumer notification of a data breach,[16] many do not yet have statutes directly governing data security practices.[17] In the absence of an overarching framework, the problem that presents itself is that a multi and cross-jurisdictional problem is treated in vastly different ways, and sometimes not addressed at all. This uncertainty creates numerous problems in a commercial world based more and more on the collection, sale, and storage of PII.

For one thing, victims of PII theft due to negligent security are often left largely without remedy.[18] Credit monitoring is generally "the universal 'band aid' offered to consumers,"[19] but it is by no means a complete solution. For one thing, credit monitoring only detects credit fraud—not the scores of other vehicles for fraud using PII—and it lasts for a finite amount of time.[20] As one senior industry analyst put it, "[b]ad guys can be very patient, so it's important to keep an eye out long after this story fades from the headlines."[21]

Conversely, holders of PII can face tremendous uncertainty with respect to their responsibility to safeguard information across jurisdictions, even in neighboring states.[22] The nature and scope of statutory duties differ, in turn

[13] Renae Merle, *After the breach, Equifax now faces the lawsuits* (Sept. 22, 2017), https://www.washingtonpost.com/news/business/wp/2017/09/22/after-the-breach-equifax-now-faces-the-lawsuits/?utm_term=.07345eb72908

[14] *See id.*

[15] CBS News, *Equifax hit with first lawsuit by U.S. city over data breach* (Sept. 26, 2017, 3:29 PM), https://www.cbsnews.com/news/equifax-data-breach-lawsuit-by-us-city/.

[16] *2018 Security Breach Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES (Feb. 27, 2018),http://www.ncsl.org/research/telecommunications-and-information-technology/2018-Security-breach-legislation.aspx.

[17] *See Cybersecurity Legislation 2017*, NAT'L CONFERENCE OF STATE LEGISLATURES (Dec. 29, 2017),http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2017.aspx.

[18] *See* Leahy, *supra* note 9, § 7 (asserting that a lack of demonstrable injury often limits the ability of plaintiffs to bring suit).

[19] *Litigation of Data Breach supra* note 9, § 7 Harm or injury required: credit monitoring.

[20] *See, e.g.*, Robert Harrow, *What For-Pay Credit Monitoring Services Actually Offer*, FORBES (Sept. 25, 2017, 10:19 AM), https://www.forbes.com/sites/robertharrow/2017/09/25/what-for-pay-credit-monitoring-services-actually-offer/ (discussing features of credit monitoring).

[21] O'Brien, *supra* note 1.

[22] *See* Leahy, *supra* note 9, § 3 (demonstrating the patchwork nature of state statutes governing data breaches).

requiring complicated compliance regimes.[23] Even before the Equifax breach, the "patchwork" of federal and state laws and regulations governing data security was "generating more interest than ever" as businesses that store consumer information wondered "how these developments should impact their data security practices."[24]

This note argues that litigants and courts should conceptualize a duty to safeguard PII under a bailment theory. Despite the relative novelty of the factual scenario, recognizing such a duty is simply a question of applying firmly established common law principles. The first such principle is the intangible property rights a person holds with respect to their PII. By definition, such information is specific to the individual and is widely recognized as being for the beneficial use of that individual as a participant in society. Next, although PII is not a tangible "thing," and certainly not a single "thing," the trust involved in giving it over to another party in order to facilitate the exchange of money for goods or services is reminiscent of a common law bailment for mutual benefit. Finally, age old principles of property law establish a duty of reasonable care with respect to the object—the breach of which gives rise to a cause of action for negligent data security.

Part II of this Note will discuss the background of data security litigation, including state and federal statutory duties, the gaps and problems associated with inconsistent treatment among these authorities, and the common law principles involved in asserting a duty to safeguard. Part III of this Note will analyze the rights individuals have in their personally identifiable information and the dynamics of the commercial bailment relationship created by the exchange of PII. Part IV will conclude by arguing that courts and litigants should conceptualize the standard cause of action for negligent data security under a quasi-bailment theory.

II. BACKGROUND

Relatively speaking, litigation of data breaches as such is still in its infancy. Thus,

> [d]espite this groundswell of potential claimants, there is no single set of laws setting forth the legal duty of care or the bases for civil liability in data breach settings. Consequently, aggrieved

[23] *See id.* ("The applicability of state and federal statutes depends on such factors as the type of data, where the data is stored, how it is stored, and who stores it. As a result, data security practices may be subject to distinct but overlapping statutory requirements.").

[24] *See* Leahy, *supra* note 9, § 3 *(*quoting Rosenfeld & McDowell, *Moving Target: Protecting Against Data Breaches Now and Down the Road*, 28-SUM Antitrust 90 (2014)).

> individuals and their attorneys have been forced to resort to a patchwork of common law and state or federal statutory claims.[25]

A. THE TYPICAL CAUSES OF ACTION

The resulting "patchwork" has worked itself out such that, at present, data breach litigation takes place on one of four planes:

I. Shareholder derivative lawsuits,
II. Securities fraud class actions,
III. Enforcement actions by governmental agencies, and
IV. Class action lawsuits by breached companies' customers or business partners.[26]

1. Shareholder Derivative Suits. Shareholder derivative actions appear in the cybersecurity/data breach context through allegations that management failed to take adequate precautions to guard against a data breach.[27] Shareholders pursuing these sorts of derivative actions face numerous challenges, including the requirement that they first make a demand on the corporation to file suit, and the judicial presumption that the decision not to do so was reasonable and made in good faith.[28] For example, Target shareholders saw their consolidated derivative suits find such an end in March 2016, after the company's appointed special litigation committee (SLC) concluded that it would not be in Target's best interest to pursue claims against the named officers and directors.[29] The shareholders stipulated to dismissal of the case in accordance with the SLC's guidelines in exchange for the right to seek attorney's fees.[30]

2. Securities Fraud Class Actions. Securities fraud class-action lawsuits have also served as a tool to recover for diminution in stock values following a cyber-breach.[31] In this context, shareholders might claim that they relied to their detriment on a company's material misrepresentations regarding data privacy or security and readiness, usually made in public statements, press releases, or the

---

[25] Michael Hooker & Jason Pill, *You've Been Hacked, and Now You're Being Sued: The Developing World of Cybersecurity Litigation*, 90 FLA. BAR J., July/August 2016 30, 31.

[26] *Id.*

[27] *Id.* at 31–32.

[28] *See, e.g.*, Palkon v. Holmes, 2014 WL 5341880 (D.N.J. Oct. 20, 2014) (dismissing a derivative suit filed against Wyndham Worldwide Corporation involving the theft of over 619,000 payment card numbers, finding the board's decision to reject the shareholder's demand to sue under the business judgement rule's presumption).

[29] Ronald W. Breaux et al., *Target Data Breach Derivative Suit Dismissed*, HAYNES BOONE (July 19,2016), http://www.haynesboone.com/alerts/target-data-breach-derivative-suit-dismissed.

[30] *Id.*

[31] Hooker & Pill, *supra* note 25.

corporation's Form 10-K reports.[32] Damages in this context manifest as a reduction in stock value, usually with the requirement by courts that there be a "statistically significant" decline in stock price.[33] In one of the earliest data breach lawsuits filed, plaintiff shareholders sued Heartland Payment Systems, Inc. in 2007 regarding a data breach impacting 130 million credit and debit card numbers.[34] Although Heartland's stock price fell almost eighty percent, and the plaintiffs alleged that the company had hidden the attack on its network and overstated its preparedness, the court dismissed the lawsuit.[35] The court held that Heartland's failure to disclose the prior cyber-attack was not a material omission, and the mere fact that the system had been infiltrated before did not necessarily mean the referenced public statements were false.[36]

3. Governmental Enforcement Actions. Federal agencies have also "gotten into the cybersecurity mix."[37] In 2014, the National Institute of Standards and Technology (NIST) released a Cybersecurity Framework,[38] which is widely considered to be the leading federal authority for cybersecurity guidance.[39] However, the Framework and related guidance are nonbinding, and provide no enforcement mechanism.[40] Thus, several other federal agencies have become active in litigating data breach issues, including the Department of Justice (DOJ), the Securities and Exchange Commission (SEC), and the Federal Trade Commission (FTC).[41]

These agencies typically rely on statutory and regulatory authority not intended for data breach litigation. In recent years, the SEC has taken steps toward pursuing more enforcement actions like regulations containing a

---

[32] *Id.* at 32.

[33] *See, e.g.*, *In re Goldman Sachs Grp., Inc. Sec. Litig.*, No. 10 Civ. 3461 (PAC), 2015 WL 5613150 (S.D.N.Y. Sept. 24, 2015), *vacated on other grounds sub nom.* Arkansas Teachers Retirement Sys. v. Goldman Sachs Grp., Inc., 879 F.3d 474 (2d Cir. 2018) (holding that defendants failed to show a complete lack of price impact due to their inability to show that the decline in stock price was attributable only to the market reaction to the announcement of enforcement actions, and not due to the material misrepresentations made).

[34] *In Re Heartland Payment Sys., Inc. Sec. Litig.*, Civ. No. 09-1043, 2009 WL 4798148, at *1 (D.N.J. Dec. 7, 2009).

[35] *Id.* at *1, *8.

[36] *Id.* at *7–8.

[37] Hooker & Pill, *supra* note 25, at 37 (noting that these initiatives have encountered "stiff resistance" due to the absence of overarching federal regulation to regulate cybersecurity, and the lack of a uniform standard for private-sector cybersecurity).

[38] National Institute of Standards & Technology, *NIST Releases Cybersecurity Framework Version 1.0* (Feb. 12, 2014), http://nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

[39] *See id.* (discussing the framework and collaboration throughout the industry); Hooker & Pill, *supra* note 25, at 37.

[40] Hooker & Pill, *supra* note 25, at 37–38 (but noting that "some commentators believe the Framework may create a de facto legal standard that ultimately is applied by the courts").

[41] *Id.* at 38.

"safeguards rule," requiring covered entities to adopt reasonable procedures for the protection of client records and information.[42]

The FTC has been even more active, bringing more than fifty enforcement proceedings relating to data security in recent years.[43] Recently, the FTC has filed lawsuits in federal court under its authority to prohibit "unfair or deceptive trade acts or practices in or affecting commerce" under § 5 of the Federal Trade Commission Act.[44] In *F.T.C. v. Wyndham Worldwide Corp.*, for example, the Third Circuit affirmed the district court's finding that differences between Wyndham's policies and practices were sufficient to support a claim under the FTCA, holding that the FTC has authority to regulate "unfair" cybersecurity failures under § 45.[45] The Court reasoned that the FTCA, along with Wyndham's prior data breach issues, provided sufficient notice of pertinent data breach standards.[46]

4. Consumer Class Actions. Finally, and most relevant to this Note, consumer class actions have continued to take shape as a form of data-breach litigation.[47] As previously noted, these actions have been asserted under statutory claims with greater and greater frequency.[48] Usage of statutory bases for suit have been numerous and varied, ranging from state statutes on point all the way to older state and federal statutes addressed toward unrelated subject matter.[49] Where statutory authority is unavailable, or simply unsuccessful, plaintiffs have turned to a number of common law theories.[50]

Some federal statutes address themselves toward data privacy and security, but even the few that codify a duty to safeguard are extremely limited in scope.[51] For example, the Gramm-Leach-Bliley Act requires financial institutions to protect consumers' nonpublic personal information, including the prevention of disclosure to unauthorized third parties.[52] However, courts have generally been unwilling to hold that other entities, like health care providers, meet the statutory criteria to be a "financial institution."[53] Along the same lines, the Fair Credit

---

[42] *See* 17 C.F.R. § 248.30 (2005); *R.T. Jones Capital Equities Management*, Proceeding No. 3-16827 (bringing charges against public companies for failure to protect the PII of customers and clients who were the victims of criminal hacking).

[43] Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 957–58 (2016).

[44] *See* 15 U.S.C. §§ 41–58 (2018).

[45] F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 243–44 (3d Cir. 2015).

[46] *Id.* at 258–59.

[47] Hooker & Pill, *supra* note 25, at 34 (also considering claims by financial institutions doing business with defendant companies).

[48] *Id.*

[49] *Id.*

[50] *Id.* at 31.

[51] *Id.* at 36.

[52] *Id.*

[53] *See id.*; *see also* Leahy, *supra* note 9, § 3 (illustrating the distinction between financial institutions and health care providers).

Reporting Act requires consumer reporting agencies to, among other things, safely dispose of consumer information and maintain reasonable procedures to avoid its disclosure.[54]

Interestingly, plaintiffs have also attempted to make use of federal statutes not aimed directly at data breach.[55] Negligence per se claims under HIPAA, for example, have achieved mixed results. In *Sheldon v. Kettering Health Network*, the Ohio Court of Appeals held that a negligence per se action under HIPAA "is no less than a private action to enforce HIPAA, which is precluded."[56] Conversely, in *Smith v. Triad of Ala.*, the court allowed the plaintiff to pursue a negligence per se action based on HIPAA based on Alabama case law "indicat[ing] Alabama courts' willingness to allow statutes that do not otherwise provide private causes of action to serve as the basis for a negligence *per se* claim. . . ."[57]

At the state level, numerous statutes have been targeted toward the duty to safeguard PII, for example:

Arkansas Personal Information Protection Act	"A person or business that acquires, owns, or licenses personal information about an Arkansas resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[58]
California	"It is the intent of the Legislature to ensure that personal information about California residents is protected. . . . A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[59]

[54] Hooker & Pill, *supra* note 25, at 36.

[55] *See, e.g.*, Complaint at 25–26, Wexler v. Peachtree Orthopaedic Clinic, No. 2016CV284076 (Ga. Super. Ct. Dec. 22, 2016) (alleging negligence per se under § 45 of the Federal Trade Commission Act, The Health Insurance Portability and Accountability Act, and the Gramm-Leach-Bliley Act).

[56] 40 N.E.3d 661, 674 (Ohio Ct. App. 2015).

[57] No. 1:14–CV–324–WKW, 2015 WL 5793318, at *12 (M.D. Ala. Sept. 29, 2015).

[58] ARK. CODE ANN. § 4–110–104(b) (2005).

[59] CAL. CIV. CODE § 1798.81.5(a)(i), (b) (West/Deering 2004).

Florida	"[e]ach covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information."[60]
Maryland Personal Information Protection Act	"To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."[61]
Maryland State Government Laws	A State government unit "that collects personal information of an individual shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information collected and the nature of the unit and its operations [to protect personal information from unauthorized access, use, modification, or disclosure]."[62]
Nevada	"A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."[63]
Rhode Island Identity Theft Protection Act of 2015	"A municipal agency, state agency or person that stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident shall implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure and to preserve the confidentiality, integrity, and availability of such information."[64]

Finally, consumer class action suits have relied on a variety of common law bases.[65] Theories include negligent misrepresentation, contractual duty,

[60] FLA. STAT. ANN. § 501.171(2) (West/LexisNexis 2014).
[61] MD. CODE ANN., COM. LAW § 14–3503 (2018).
[62] MD. CODE ANN., STATE GOV'T § 10–1304 (2018).
[63] NEV. REV. STAT. § 603A.210(1) (2018).
[64] 11 R.I. GEN. LAWS § 11–49.3–2(a) (2015).
[65] Hooker & Pill, *supra* note 25, at 34.

equitable theories, and, of course, common law negligence.[66] Each of these first four theories faces procedural challenges that—although there may be isolated situations in which a claim is viable—make them of little help to the bulk of plaintiffs. Negligent misrepresentation claims, for example, require overt representations by a defendant that they "would take reasonable measures to protect the plaintiff's information."[67] Even where a plaintiff can show such a representation, defendants can escape these claims by demonstrating reliance on the representation was not justified.[68] Similarly, it has been difficult to establish even implied contractual agreements to safeguard PII,[69] particularly where the parties do not share a direct relationship.[70]

In at least one case, a court has accepted equitable theories like unjust enrichment as stating a claim for recovery of damages related to a data breach. Among the theories surviving the motion to dismiss in *In re Target Corp. Customer Data Security Breach Litigation*[71] was the plaintiff's unjust enrichment "would not have shopped" theory.[72] The *Target* court held that

> [i]f Plaintiffs [could] establish that they shopped at Target after Target knew or should have known of the breach, and that Plaintiffs would not have shopped at Target had they known about the breach, a reasonable jury could conclude that the money Plaintiffs spent at Target is money to which Target "in equity and good conscience" should not have received.[73]

The court did, however, reject the plaintiffs' "overcharge" theory, reasoning that the plaintiffs could not plausibly allege that they had been overcharged to

---

[66] *Id.*

[67] *Id.*

[68] *See, e.g.*, *In re* Heartland Payment Sys's Inc. Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566, 590 (S.D. Tex. 2011) (dismissing plaintiff's negligent misrepresentation claim for failure to prove reliance was reasonable), *rev'd in part on other grounds sub nom.* Lone Star Nat. Bank, N.A. v. Heartland Payment Sys's, Inc., 729 F.3d 421 (5th Cir. 2013) (interpreting New Jersey law and reversing and remanding on plaintiffs negligence claim).

[69] *See, e.g.*, Resnick v. AvMed, Inc., 693 F.3d 1317, 1325 (11th Cir. 2012) (alleging, *inter alia*, a breach of a contract to provide healthcare by allowing unauthorized access to medical information); *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 118 (D. Me. 2009) (alleging breach of a contract to protect customer's debit card information implied in a contract for the sale of goods), *aff'd in part, rev'd in part sub nom.* Anderson v. Hannaford Bros. Co., 659 F.3d 151 (1st Cir. 2011).

[70] *See, e.g.*, Hammond v. Bank of N.Y. Mellon Corp., No. 08 Civ. 6060(pmb)(RLE), 2010 WL 2643307, at *9–11 (S.D.N.Y. June 25, 2010).

[71] 66 F. Supp. 3d 1154 (D. Minn. 2014).

[72] *Id.* at 1178.

[73] *Id.*

offset the costs of data security since cash customers paid the same price and faced no risk of PII theft.[74]

In recent years negligence has picked up speed as the theory of preference in consumer class actions.[75] Even so, there appears to be relatively little exploration of the nature and source of the duty to safeguard. In some respects this is unsurprising, and yet even when a plaintiff can meet his burden to show breach, cause, and harm, the question of whether and why a defendant has the duty to safeguard has proved to be surprisingly recalcitrant. There are a handful of possible explanations for the absence of discussion on the *basis* for a duty to safeguard.

First and foremost—these cases are relatively new, and they are not inherently "high-dollar" claims.[76] In terms of the development of the law, one might conclude there simply has not been enough time for appellate courts to hear and decide the issue.

Second, in many cases the question is simply not considered in great detail. For example, in 2014 the District Court for Minnesota considered numerous theories purporting to state a data breach claim, but, for the purposes of the motion, Target did not dispute that Plaintiffs had plausibly alleged the existence of a duty to safeguard. Instead, the company chose to argue that the plaintiffs had failed to allege any damages and that the negligence claims were barred by the economic loss rule.[77]

Relatedly, and as *Target* illustrates, there are significant procedural hurdles to recovery that garner more attention from courts and litigants. Most notably, data breach plaintiffs have difficulty making adequate showings of standing and harm.[78] Courts have often held that data breach plaintiffs lacked standing to sue because "no actual harm has occurred."[79] The typical reasoning in these cases is that damages are not recoverable on the mere *possibility* of identity theft because of the lack of proof of actual injury.[80] Thus, arguments around standing and harm are typically the focus of dispositive motions and orders, so that

---

[74] *Id.*

[75] David Zetoony et. al., *2017 Data Breach Litigation Report: A comprehensive analysis of class action lawsuits involving data security breaches filed in United States District Courts*, BRYAN CAVE LEIGHTON PAISNER (Sept. 8, 2017), https://www.bryancave.com/images/content/9/6/v2/96690/Bryan-Cave-Data-Breach-Litigation-Report-2017-edition.pdf

[76] *See* John P. Hutchins & Renard C. Francois, *A New Frontier: Litigation over Data Breaches*, 20 No. 4 Prac. Litigator 47 (2009) (discussing the litigation landscape for data breaches).

[77] *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014).

[78] *See* Leahy, *supra* note 9, § 7.

[79] *See id.*

[80] *See*, *e.g.*, *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 4 A.3d 492, 496 (Me. 2010) (finding that time and effort, spent to avoid or remedy foreseeable harm was not a cognizable injury for which damages could be recovered under the law of negligence).

relatively little thought is given to *why* holders of PII have a responsibility to safeguard it in the first place.

B. THE QUASI-BAILMENT THEORY

Interestingly, relatively few data-breach consumer plaintiffs have asserted claims based on bailment theories.[81] With only minor variations in language across jurisdictions, the elements of a bailment are:

> (1) delivery of personal property by one person to another to be used for a specific purpose;
>
> (2) acceptance of such delivery; and
>
> (3) an express or implied contract that the purpose will be carried out and the property will then be returned or dealt with as otherwise directed.[82]

This definition of a bailment under Texas state law largely tracks the language found in legal encyclopedias and practice manuals:

> A bailment is a contractual relationship, express or implied, which results from the delivery of personal property by one person . . . and an acceptance of the property by another . . . for the accomplishment of some purpose, beneficial to either the bailor or bailee or both, on the condition that, once the purpose has been fulfilled, the bailed property must either be redelivered to the bailor, kept until he reclaims it, or otherwise dealt with according to his directions.[83]

Naturally, there are potential roadblocks to the use of a bailment theory in the data breach. First and foremost, it is not immediately clear that PII is the type of "object," if indeed it is an object, which might be the subject of a bailment. Second, it is not obvious that "the shoe fits" for a bailment theory, since bailments typically require return of the bailed object. Third, questions might reasonably arise as to the very existence of an agreement, express or

[81] *See* Zetoony, *supra* note 75 (charting the statistical breakdown of theories utilized by plaintiffs' attorneys in data breach litigation complaints, and showing that only 18% of complaints include a bailment claim, compared to 95% including negligence claims)

[82] Lynch Props. Inc. v. Potomac Ins. Co. of Ill., 140 F.3d 622, 627 (5th Cir. 1998).

[83] Mark S. Dennison, *Bailee's Liability for Damage, Loss, or Theft of Bailed Property*, 46 Am. Jur. Proof of Facts 3d 361, § 2: Creation of Bailment Contract; Delivery and Acceptance (updated Feb. 2018).

implied, giving rise to the bailment. The data-breach case law evaluating the bailment theory reflects these concerns.

Of the cases dealing with data breach litigation on a bailment theory, *In re Sony Gaming Networks & Customer Data Security Breach Litigation*[84] appears to have done so in the most detail. The court identified three failings in the bailment theory. First, the plaintiffs alleged only that Sony failed to maintain reasonable data security, and thus "there [were] no allegations of conversion or any other intentional conduct by Sony that would indicate that Sony sought to unlawfully retain possession of Plaintiffs' Personal Information."[85] Second, the court declared itself "hard pressed to conceive of how Plaintiffs' Personal Information could be construed to be personal property so that Plaintiffs somehow 'delivered' this property to Sony and then expected it be returned," and that, in any event, "if such a legal theory for bailment exists, Plaintiffs have failed to present the Court with such in its Opposition papers."[86] Finally, the court found the bailment claim duplicative of the claims for negligence and violation of California consumer protection statutes, such that "any damages Plaintiffs might be able to recover under this unorthodox claim for bailment would be recoverable under its negligence and/or consumer protection claim."[87]

Relying on *Sony* in part, the District Court for Minnesota found fault in the consumer-plaintiffs' bailment claim in *Target* because "[e]ven if Plaintiffs are correct that intangible property such as their personal financial information can constitute property subject to bailment principles, they [did] not—and [could not]—allege that they and Target agreed that Target would return the property to them."[88]

Finally, the Court in *Enslin v. Coca-Cola Co.*[89] considered the bailment issue only in sufficient detail to note that "courts in Pennsylvania have yet to consider whether such a claim could arise in connection with a loss of electronic information," and agreed with the logic of *Sony*, *Target,* and *Ruiz*, on the belief that "Pennsylvania courts would do the same."[90]

Thus, courts have found four types of problems with bailment theories in the data breach context. First, reasonable questions might be raised about the express or implied creation of the bailment relationship itself. Second, some courts have expressed concern about whether PII is personal property for the purposes of being delivered and returned in a bailment relationship. Third,

84 903 F. Supp. 2d 942 (S.D. Cal. 2012).

85 *Id.* at 974.

86 *Id.*; *see also* Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008) (holding that social security numbers and credit card information stolen from a computer were not property for purposes of the law of bailment).

87 903 F. Supp. 2d at 974–75.

88 66 F. Supp. 3d at 1177.

89 136 F. Supp. 3d 654 (E.D. Pa. 2015).

90 *Id.* at 679.

courts have shown a recurring concern with holding a bailee liable for breach of bailment when the damage is done by third-party criminal activity. Finally, courts have expressed doubt about the bailment theory of data breach on the ground that PII cannot be "returned" in the ordinary sense of bailed objects, and therefore possession is not properly "temporary." Part III will analyze these and related issues involved in establishing a quasi-bailment theory giving rise to a duty to take reasonable care to safeguard PII.

III. ANALYSIS

Courts should conceptualize data breach litigation under the framework of a quasi-bailment theory.

> A bailment is a contractual relationship, express or implied, which results from the delivery [and acceptance] of personal property. . . for the accomplishment of some purpose, beneficial to either the bailor or bailee or both, on the condition that, once the purpose has been fulfilled, the bailed property must either be redelivered to the bailor, kept until he reclaims it, or otherwise dealt with according to his directions.[91]

While negligence claims are the most common claim asserted in data breach cases,[92] this theory of data breach largely fails to explain *why* the duty exists. By contrast, a bailment theory clearly explains why the duty exists, and thereby informs its parameters and the relevant inquiries. In this context, an implied bailment may be created via the delivery and acceptance of PII in a commercial exchange for the purpose of facilitating the exchange, creating a mutually beneficial relationship with the customarily implied condition that the PII will be used for the purposes of the relationship and safeguarded against theft. While the PII may not be "returned" as such, the bailee deals with it according to implied instructions to use it as agreed, safeguard it, and subsequently store or dispose of it by reasonable means.

A. INDIVIDUALS HAVE A PROPERTY INTEREST IN THEIR PII

It should be noted at the outset what this argument is *not*: the argument is *not* that individuals *own* their personally identifiable information, at least not in any sense that involves exclusivity and exclusion. What the argument *is*, is that individuals have a property interest in the security of their PII. This is seen in both the theoretical underpinnings of property law and the current state of the

[91] Dennison, *supra* note 94.

[92] Zetoony, *supra* note 75

law today. On a theoretical basis, common law utilitarian principles and Lockean theory support the assertion that individuals have an interest in their PII. Further, the law presently contains numerous positive protections of PII,[93] all of which are consistent with an individual's interests in their PII for the purposes of a bailment.

1. Individuals clearly do not "own" their personally identifiable information. This much is clear from case law addressing claims that ownership of PII gives a person exclusionary rights to prevent information traders from dealing in PII itself.[94] Such claims advance ownership and interest theories aimed at information *privacy*. Along these lines, "[p]ractically all federal and state laws that address the issue of individual consent [to the collection of PII] apply the 'opt-out' rule" requiring companies to allow individuals the opportunity to opt out of standard information practices, as opposed to the "opt-in" model, "which obligates companies to obtain express consumer consent before they can share or sell [customer PII]."[95]

However, American law dealing with PII is "'a patchwork of uneven, inconsistent, and often irrational' federal and state rules."[96] Most such rules protecting individuals from dissemination of their personal information apply only to government entities,[97] and the few federal regulations covering the transfer of PII in the private market are industry- and even situation-specific.[98] Importantly, "these regulations are not based on any uniform theory of rights."[99] Thus, as clear as it is that individuals do not own their PII, it is equally clear that

[93] *See, e.g.*, Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2383–84 (1996) ("[P]ersonal information [is] any data about an individual that is identifiable to that individual . . . . Such information, like all information, is property.").

[94] *See, e.g.*, Shibley v. Time, Inc., 341 N.E.2d 337, 340 (Ohio Ct. App. 1975) (rejecting a subscriber's claim for unauthorized sale of subscriber lists); *see also* U.S. News & World Report, Inc. v. Avhrami, No. 95-1318, 1996 Va. Cir. LEXIS 518, at *16–17 (Va. Cir. June 13, 1996) (rejecting claims seeking to block unauthorized dissemination of PII based on a theory of misappropriation of one's name because individuals do not have property rights in the names they use).

[95] *See* Bergelson, *supra* note **Error! Bookmark not defined.**, at 393.

[96] *See id.* at 391 (quoting FRED H. CATE, PRIVACY IN THE INFORMATION AGE 80 (1997)).

[97] *See id.*; *see, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552(a) (2000) (permitting individuals to determine which personal records are collected, maintained, or disseminated by federal agencies); *see also* Right to Financial Privacy Act, 12 U.S.C. §§ 3401–(2000) (providing procedural requirements for sharing financial information among federal agencies).

[98] *See* Bergelson, *supra* note **Error! Bookmark not defined.**, at 391–92; *see, e.g.*, Fair Credit Reporting Act of 1970, 15 U.S.C.S. 1681 (2002) (recognizing the individual's right to privacy with regard to disclosure of credit records); Right to Financial Privacy Act, 12 U.S.C.A. §§ 3401–3404 (2002) (recognizing individual's right to privacy with regard to disclosure of financial records by banks and governmental agencies).

[99] *See* Bergelson, *supra* note **Error! Bookmark not defined.**, at 392.

the law does not foreclose the possibility that individuals may have a property interest in the security of their PII.

An individual's property interests in PII security should *not* be foreclosed by these rules ,because the impetus behind most information privacy laws simply does not carry over. Considering PII rights in reference to data security, it makes sense to recognize greater property interests. In the privacy context, the notion is that individuals have *exclusionary* rights to their PII, i.e., commercial entities may not disseminate the information without that person's consent.[100] At its heart, this is a pretty expansive claim. Exclusionary rights over who may "possess" information like one's name, home address, and date of birth would involve a level of control over information far and above even the most liberal rights of publicity. Claims to property interests in PII for security purposes, however, are not nearly so expansive.

2. More to the point, utilitarian principles would seem to support the assertion that individuals have an interest in the security of their sensitive PII. "Under the utilitarian theory, rights should be allocated so as to maximize human satisfaction or benefit."[101] In recent years, this has been interpreted to mean economic efficiency and the facilitation of wealth-maximizing transactions.[102] Unlike information privacy, it seems clear that the security of sensitive personal information is the more efficient outcome.

By way of example, Judge Posner concluded in his article "The Right of Privacy" that the efficient outcome in the privacy context is to assign the property right to the seller of PII, rather than the individual.[103] It is doubtful, however, that his rationale translates to the security context. Judge Posner reasoned that, for purposes of company's commercial use of consumer information, "the cost of obtaining the subscriber's approval would be high relative to the low value of the list."[104] Although there is some dispute on the specifics of that claim,[105] the logic itself appears to be sound. This same logic does not apply, however, to PII in the security context. Simply put, lax data security is almost certainly inefficient.

---

[100] *See, e.g.*, Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECHN. 91 (2009) (examining the nature of data collection and dissemination).

[101] Bergelson, *supra* note **Error! Bookmark not defined.**, at 421, *citing* JEREMY BENTHAM, 1 SELECT EXTRACTS FROM THE WORKS OF JEREMY BENTHAM 33 (Thoemmes Press 1995) (1843).

[102] *See* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 36–39, 271–89 (4th ed. 1992); Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243, 1244–45 (1968).

[103] Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 398 (1978).

[104] *Id.*

[105] *See* Bergelson, *supra* note **Error! Bookmark not defined.**, at 421–22 (citing studies by Kenneth C. Laudon indicating the inefficiency involved with telemarketers and junk-mail).

Take the Equifax breach. On September 7, 2017, Equifax announced it had suffered a massive breach that "compromised the personal information of as many as 143 million Americans—almost half the [adult population of the] country."[106] Examples of subsequent inefficiencies—be they temporal or monetary—are legion. Equifax's website and phone systems were apparently so heavily bogged down in the days and weeks after the breach that it was extremely difficult for affected persons to obtain information about the breach, determine whether or not they were affected, and find out what to do next.[107] Apparently, Equifax's responsiveness became so bad that people began to wonder if the company was deliberately obfuscating attempts to obtain credit freezes.[108] Equifax representatives eventually told reporters that the company was experiencing such a high volume of requests and communications that, on top of everything else, Equifax was experiencing technical difficulties in responding.[109] Those customers that were able to get through to Equifax found that many representatives had outdated information about the breach, if they had any at all.[110] This required Equifax to spend still more time and money training its troubleshooting team.[111]

Even when customers were able to freeze their credit, many experienced difficulties in obtaining the PIN number necessary to unfreeze their credit later on.[112] While Equifax maintained many of these issues were browser errors, the fact remained that it became necessary to set up mechanisms to verify identities by phone and generate new PINs, and even consider sending PINs via post mail instead.[113]

It is axiomatic, on the other hand, that "[d]ata breaches are, at least to some degree, preventable" and "[t]o the extent they are not preventable, their effects can be mitigated by the way the company whose data is breached handles the breach."[114] FTC guidelines are instructive on this point:

The Federal Trade Commission [has been] concerned with at least five inadequate data security practices:[115]

106 O'Brien, *supra* note 1.

107 Ron Lieber, *Equifax Finally Responds*, N.Y. TIMES, Sept. 14, 2017, at B1.

108 *Id.*

109 *Id.*

110 *Id.*

111 *Id.*

112 *Id.*

113 *Id.*

114 Leahy, *supra* note 9, § 2 (citing Dave Maxfield & Bill Latham, *Data Breaches*, 25 S.C. LAW. 28, 30 (2014)).

115 *Id.* (citing Abraham Shaw, Note, *Data Breach: From Notification to Prevention Using PCI DSS*, 43 COLUM. J.L. & SOC. PROBS. 517, 558–59 (2010).

> 1. Inadequately assessing system vulnerability to commonly known or reasonably foreseeable attacks.
>
> 2. Failing to apply low-cost, simple, and readily available defenses.
>
> 3. Using default user ID or passwords to protect sensitive data rather than stronger passwords to prevent hackers.
>
> 4. Storing information in unencrypted files and sending sensitive data via unencrypted transmission routes.
>
> 5. Failing to develop unauthorized access detection mechanisms.

While there is undoubtedly cost and time consumption associated with correcting these practices, it appears to be generally true that they are achievable within reason. The salient detail, therefore, is that "[i]f not prevented or mitigated, data breaches can cause enormous harm and result in significant financial damages."[116]

On balance, therefore, negligent data security is inefficient, and utilitarian principles counsel imposing a duty to safeguard.

3. More importantly still, the law confers or recognizes confidentiality rights in PII in numerous and varied contexts. First, and most notably, HIPAA imposes strict confidentiality requirements on the use of a person's medical information.[117] Title II of HIPAA establishes policies and procedures for maintaining the privacy of health related PII.[118] The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information held by "covered entities," including employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.[119] While covered entities may disclose information for law enforcement purposes or to facilitate treatment, payment, or health care operations, disclosures of Personal Health Information generally require written authorization from the individual for the disclosure.[120]

Similarly, under the Health Information Technology for Economic and Clinical Health Act (HITECH), the United States Department of Health and Human Services (HHS) promoted and expanded the adoption of health

---

[116] *Id.*

[117] *Id.* § 3 n.6.

[118] *See generally* Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, August 21, 1996, 110 Stat. 1936.

[119] 45 C.F.R. §§ 164.502, 160.103 (West 2018).

[120] 45 C.F.R. 164.502(a)(1)(iv).

information technology.[121] In relevant part, the HITECH Act requires entities covered by the HIPAA to report data breaches which affect 500 or more persons to HHS, the news media, and persons affected by the data breaches.[122]

Finally, the confidentiality interests established in HIPAA, the Code of Federal Regulations, and HITECH also find analogues at the state level in the many varieties of data-breach notification statutes mentioned above.[123] Thus, in these types of statutes, the law already recognizes the existence of confidentiality and security interests in personally identifiable information. Based on these examples, it is not a stretch to conclude that PII may be the type of property that can be the object of a bailment.

B. COMMERCIAL TRANSACTIONS INVOLVING PII MAY PLAUSIBLY INVOLVE A BAILMENT AGREEMENT

While some courts have expressed concern about establishing the existence of a bailment agreement,[124] commercial transactions involving PII commonly involve at least a plausible allegation of an implied bailment agreement. For one thing, the public outcry *routinely* observable after a large-scale data breach suggests that the general public understands the commercial holder to have a duty of reasonable care. More importantly, however, courts have begun to recognize that the realities of modern life imply a promise to safeguard PII.[125]

In *Daly v. Metropolitan Life Ins. Co.*, for example, the Supreme Court of New York found that a purchaser of life insurance "was required to, and agreed to, supply Met Life with highly sensitive personal information including her full name, her Social Security number, and her date of birth," concluding "[i]mplicit in this agreement was a covenant to safeguard this information."[126] The court explained:

> The gravamen of plaintiffs' claims is that, in order to obtain a life insurance policy, Ms. Daly had to provide sensitive personal information for herself and for her father. Met Life represented that this information would be protected and would remain fully

[121] *See, e.g.*, U.S. Dep't of Health and Human Services, *HITECH Act Enforcement Interim Final Rule*, https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html (last visited Mar. 19, 2018).

[122] 42 U.S.C. § 17932(e) (2010).

[123] *See supra* text accompanying notes 58–71.

[124] *See* discussion *supra* Section II.B.

[125] *See* 4 Misc. 3d 887, 893 (Sup. Ct. N.Y. 2004); *see also* Jones v. Commerce Bancorp, 2006 U.S. Dist. LEXIS 32067 (S.D.N.Y. May 23, 2006).

[126] 4 Misc. 3d 887, 893 (Sup. Ct. N.Y. 2004).

> confidential. Relying on that promise, Ms. Daly released her personal information.[127]

This summary explains the paradox of refusing to recognize a duty to safeguard under the quasi-bailment theory: people engage in numerous PII-dependent transactions every day, many of them realistically less optional than the decision to purchase life insurance, which require them to trust another person with their PII. Common experience would seem to reflect that consumers and commercial entities understand there to be an implied covenant to keep the data secure.

Thus, the *Daly* court noted, "[p]laintiffs' claims are similar to those seen in causes of action for breach of fiduciary duty of confidentiality."[128] The court further explained that, within the doctor-patient relationship, this duty comes "not . . . from a statutory right . . . [but] from 'the implied covenant of trust and confidence that is inherent in the physician patient relationship. . . .'"[129] And, indeed, "[a] similar covenant of trust and confidence may be inferred in business dealings."[130] The court concluded that "this concept has never before been applied to issues surrounding the protection of confidential personal information, [but] perhaps in the absence of appropriate legislative action, it should."[131]

It should. Both customers and businesses undoubtedly recognize the gravity of a data breach and the harm that flows from it. And it is entirely plausible that, in light of this reality, under some circumstances this understanding takes the next step into being an implied promise to keep and use PII safely, within reason.

The substance of the agreement, moreover, need not be excruciatingly explicit to be discernible. On its own terms, a bailment for mutual benefit requires only that the bailee exercise reasonable care in safeguarding the object of the bailment.[132] While "reasonable" data security is undoubtedly a fact specific question, there are certainly reasonable starting points available in the data-breach literature:

Security failures resulting in loss of data include:

> (a)Failing to establish or enforce rules sufficient to make user credentials hard to guess. For example, customers may be allowed to use the same word, including common dictionary

127 *Id.* at 892.

128 *Id.*

129 *Id.*

130 *Id.*

131 *Id.*

132 *See* Dennison, *supra* note 83, §§ 4–5.

> words, as both the password and user ID, or a close variant of the user ID as the password.
>
> (b)Permitting the sharing of user credentials among a customer's multiple users, thus reducing likely detection of, and accountability for, unauthorized data searches.
>
> (c)Failing to require periodic changes of user credentials, such as every 90 days, for customers with access to sensitive, nonpublic information.
>
> (d)Failing to suspend user credentials after a certain number of unsuccessful log-in attempts.
>
> (e)Allowing customers to store their user credentials in a vulnerable format in cookies on their computers.
>
> (f) Failing to require customers to encrypt or otherwise protect credentials, search queries, and/or search results in transit between customer computers and Web sites.
>
> (g)Allowing customers to create new credentials without confirming that the new credentials were created by the customers rather than identity thieves.
>
> (h)Failing to adequately assess the vulnerability of the web application and computer network for commonly known or reasonably foreseeable attacks.
>
> (i)Failing to implement simple, low-cost, and readily available defenses to these attacks.[133]

The virtue of this approach is threefold. First, the analysis lends itself to flexible application to the varying size of PII holders, the amount of information they store, and even the range of PII involved in their business. Second, while a "reasonable care" standard does not provide quantifiable clarity in data security standards, it imposes a framework that is familiar to corporate litigants, conducive to presenting defenses to liability in court, and will foster consistency across jurisdictions. Finally, a duty to safeguard based on a bailment theory does not automatically equate the possession of another's PII with the duty to

[133] *See* Leahy, *supra* note 9, § 2 (citing NIMMER & TOWLE, LAW OF ELECTRONIC COMMERCIAL TRANSACTIONS § 16.06(1)(B)).

safeguard it; instead, it offers a workable framework for rendering consistent decisions on when the duty exists and how far it goes. In this sense, the bailment theory is a preferable alternative to other proposed regimes.[134]

C. PROTECTING PII AGAINST THIRD-PARTY CRIMINAL ACCESS FALLS WITHIN THE SCOPE OF THE IMPLIED BAILMENT AGREEMENT

Fundamentally, the duty of care under a bailment theory includes "safeguarding the bailor's property . . . for any damage, loss or theft proximately caused by his lack of reasonable care.[135] There is no particular reason this should not apply to data breach litigation, and numerous reasons it should.

To begin with, the analogy plays. It is universally true in bailment law that the nature of "reasonable" care requires analysis on a case-by-case basis.[136] This is no less true in data breach than with regard to tangible objects. In the bailment of tangible objects, a good example might be the theft of a bailed vehicle from a bailee's parking lot. In that case, relevant considerations include factors like whether there were enough parking lot attendants on duty or whether it was reasonable to leave the vehicle unlocked with the keys inside.[137]

It is not difficult to analogize the parking lot to a server, nor PII to the cars. Granted, the functionality of the exchange is not a perfect match—but it doesn't have to be. The purpose of the analogy is to show that data security may also be unreasonable if it lacks "enough parking lot attendants," i.e., "inadequately assess[es] system vulnerability to . . . reasonably foreseeable attacks," or "fail[s] to apply low-cost, simple, and readily available defenses,"[138] or else "leaves the keys in an unlocked car," i.e., "stor[es] information in unencrypted files," or "fail[s] to develop unauthorized access detection mechanisms."[139]

In the context of these commercial relationships built on PII, the very nature of an implied bailment agreement is that an individual gives over control of their information (or at least that compilation of it) to a commercial entity in order to obtain services with the understanding that it will be used for that purpose and

---

134 *Contra* John A. Fisher, *Secure My Data or Pay the Price: Consumer Remedy for The Negligent Enablement of Data Breach*, 4 WM. & MARY BUS. L. REV. 215 (2013).

135 *See* Dennison, *supra* note 83, § 11.

136 *See id.*

137 *Id.* (citing Allright Parking System, Inc. v. Deniger, 508 S.W.2d 127 (Tex. Civ. App. Eastland 1974) ("[F]inding that bailee did not exercise reasonable care to protect bailor's car against theft because parking lot was not attended by an adequate and prudent number of employees."); Schulze v. Allison, 204 Okla. 147, 227 P.2d 658 (1950) ("[F]inding that bailee failed to use reasonable care to protect bailed vehicle from theft where single attendant on duty was required to park and deliver cars of customers from connecting parking lots and left keys in ignition.").

138 Leahy, *supra* note 9, § 2.

139 *Id.*

protected against others. The implied bailment agreement itself centers around the protection of PII against unauthorized access.

D. WHILE A BAILEE CANNOT "RETURN" PII IN THE ORDINARY SENSE, THE BAILEE RETAINS OR DISPOSES OF THE PII ACCORDING TO CONDITIONS OF THE BAILMENT IMPLIED IN CUSTOM

Admittedly, a bailee cannot "return" PII in the customary sense of presenting the bailor with the object and relinquishing its control to the bailor. However, this cannot defeat a quasi-bailment of PII because, as noted above, a bailee must either return the bailed property to the bailor, or dispose of it according to his instructions.[140]

It is worth reiterating that the principle concern of returning a bailed object to the bailor is not any rigid or formalistic concern for technicality, but rather clearly demonstrating that the object in question is *bailed*—rather than given. The guiding principle in a quasi-bailment, therefore, should be some similar requirement that the original conveyance does not pass title nor surrender the property. This is clearly met in the PII context.

Firstly, conveyance of PII to the bailee clearly does not sever the bailor's interest, because in every instance the bailor's confidentiality interest in the PII remains unchanged. The bailor has in no sense passed title or otherwise relinquished his interest in his personally identifiable information. Any such suggestion would be absurd—notice statutes, confidentiality requirements, and the broader world of privacy and nondisclosure operate where a person or entity holds another person's PII.

Similarly, the nature of the transaction is such that the bailee has clear, although implied, instructions as to how to handle PII. Namely, it is reasonable to say that customary usage of PII establishes the parties' shared expectation that, during the course of the relationship, the bailee is to use the information for the agreed purpose, reasonably protect it against unauthorized access, and return it thereafter or dispose of it according to customary practice. In this sense, the implied instructions as to the PII may be thought of in one of two ways: an indefinite bailment or a bailment ending upon safe disposal.

In the first alternative, the bailment may simply be thought of as lasting for an indefinite term. While the concept is admittedly somewhat novel, it makes sense in the PII context in a way it simply could not with tangible objects. A tangible object must be returned within some definable length of time, or for all intents and purposes it effectively becomes the property of the bailee. Not so with PII. No matter how long a data collector, retailer, or healthcare provider stores PII, it never becomes any less personal to the bailor, and his interest in it does not diminish until his death. Further, because the bailee must also store

[140] *See* Dennison, *supra* note 83.

and protect the information of *present* customers, it might not unreasonably heighten the burden of the bailee to be held to his agreement.

Conversely, the bailment may also be terminated upon the safe disposal of the information. In the paper era of information storage, at some point it became necessary to physically dispose of older records no longer in use. While storage capacities for digital information exponentially exceed the capabilities of paper storage, companies may choose to dispose of non-current records for any number of reasons. Once a bailee safely wipes the information from his digital records, he is absolved of any duty to safeguard that particular manifestation of PII. And again, disposal of the information instead of per se "return" does nothing to diminish the bailor's interests in or value derived from PII, so the purposes of temporary conveyance are served.

Thus, plaintiffs in data breach cases might plausibly state a claim for negligent data security under a quasi-bailment theory.

IV. CONCLUSION

If recent experience has taught us anything, it is that data breach concerns are likely to become more pressing, not less. The patchwork legal framework for imposing varying duties under varying circumstances across state lines not only deprives plaintiffs of a remedy, but imposes complicated compliance regimes for commercial PII holders.

At bottom, the thrust of this Note is this: quasi-bailment theories imposing a duty to safeguard PII may state a claim sufficient to surpass a motion to dismiss. Undoubtedly, the circumstances of a given case may prevent a claim from reaching the requisite plausibility—and the facts of many cases will certainly make it difficult to survive summary judgement—but modern usage of PII and common law bailment principles lead one to conclude that commercial holders of PII may have a duty of reasonable care to protect that information against third-party criminal theft.

At a broad level, this is a problem for the courts, not the legislature. Despite the modernity of the problem, the solution is better vested in a system that adjudicates on a case-by-case basis and can therefore evaluate each case based on security standards that are reasonable at the time. This is because in one sense, the data breach problem is more like an arms race than a bank robbery: a legislature may simply make theft illegal, but the nature of data theft and security is that methods and techniques are constantly evolving in response to one another, at a pace which neither the legislature nor an administrative agency can hope to match.

Moreover, this is simply not a field where "one size fits all" security standards fairly asses when security is reasonable or not. Firms collecting PII have varying levels of resources, store varying amounts and types of PII, and face different levels of threats. Thus, what administrative agencies like the FTC might do

instead, for example, is study common data security practices that will help courts establish guidelines within which changing practices and technologies may fit.

Therefore, it is far better that we instruct commercial holders of PII to exercise reasonable care when their possession of PII stems from a quasi-bailment, and allow them to defend themselves on those terms if a breach occurs. Admittedly, this does not totally resolve the uncertainty that businesses face. What it does do, however, is bring uniformity and familiarity to *how* questions of negligent security will be addressed, while still allowing for the necessary flexibility in *what* those questions will be. From the perspective of consumer class actions, this is a marked improvement.

Indeed, the alternative seems to be a rigid statutory framework that inevitably fails, to the extent it tries, to mandate data security standards that are *not* one size fits all. Under the proposals in this Note, the holder can present evidence rebutting the presumption of such an agreement, assert procedural defenses like standing and harm, and, of course, argue that their security measures were reasonable.