Santa Clara High Technology Law Journal

Volume 36 | Issue 2 Article 1

2-4-2020

CYBERDAMAGES

Black, Stephen T.

CYBERDAMAGES

By Stephen T. Black[1]

Theft of personal property is easy to consider, but theft of information poses unique problems. Courts and legislatures dealing with victims of data breaches grapple with whether the victim has been harmed – in a manner that the law can redress. In most cases, the thief is gone, and the victims – the individual whose data was taken and the company it was entrusted to – are engaged in a lawsuit. This article engages in a discussion on the nature of such "cyberdamage," and whether a mere showing of damage to privacy is enough, or if a showing of financial harm is required.

CONTENTS

[1] Visiting Professor of Law, University of Houston Law Center; Professor of Law, Texas Tech University School of Law; LL.M. Taxation, University of Washington School of Law (2000); J.D., J. Reuben Clark School of Law, Brigham Young University (1994); B.S., Brigham Young University (1988). The author gratefully acknowledges the financial support of the Texas Tech University School of Law for this Article.

INTRODUCTION

When an individual steals from you, the damage you suffer comes in many forms, including the loss of property, a feeling of violation and invasion of privacy, and a resultant perception of being vulnerable. While the legal system measures the economic loss from theft, it does not measure well (if at all) the damage due to nonfinancial factors. For example, replacement value, increased insurance risk and costs paid for additional security may be recovered.

Theft of personal data is a growing frontier, both for criminals and companies seeking to protect data. When an individual takes personal data,[2] either from you or from a third party you have entrusted it to, does the legal system interpret that as theft? Part of the difficulty plaintiffs have faced is defining the nature of the harm they suffer when a company does not protect their information. Is this an invasion of privacy? A tort of negligence? A breach of trust? A crime?

In examining these questions, this article will start with the law of theft, particularly as it applies to information theft, and then proceed to look at the law of torts. We will then discuss the nature of personal information, what the law perceives as damages from the misappropriation of that information, and how the courts are dealing

[2] Laws in the United States usually refer to this data as "personally identifiable information" (PII), while other nations may reference "personal data", "personal information" or "important data."

with the ever-growing number of class action suits due to data breaches.

I. THE LAW OF THEFT

A. What is "Theft?"

The colloquial term "theft" refers to crimes involving the taking of a person's property without their permission. But theft in the legal sense may encompass more than one category of crime, and sometimes more than one level of seriousness. In both usages, we can start with the definition of theft as the unauthorized taking of property from another with the intent to permanently deprive them of it.

Within the taking element, we can talk about the mechanics of seizing possession of property, including removing or attempting to remove the property from another's possession. However, it is frequently the element of intent where most of the complex and interesting legal questions typically arise.[3]

Example 1. Tara walks by a bicycle on the street. She takes the bicycle with the intent of keeping it.

Example 2. Tara is working on a computer at the library and sees a flash drive that is not hers at the workstation. She picks it up, puts it in her pocket, and walks out the door with the intent of keeping it.

What has Tara stolen? The bicycle is an easy case, as is the actual, physical flash drive. But what if Larry is a photographer, and the flash drive contains Larry's latest photos?

> "At early common law, the subject of larceny was limited to tangible personal property, such as cash, jewelry, furniture, and other merchandise. The requirement of asportation excluded from the protection of theft law things at two ends of the property continuum: at one end, real property; at the other, intangible property such as choses-in-action, stocks, and bonds."[4]

B. Theft of Intangibles

Historically, the law would not have considered Larry the victim of theft of his photos because it was not tangible. But looking at the situation today, we would consider the loss of the flash drive to be de

---

[3] *Theft Overview*, FINDLAW, https://criminal.findlaw.com/criminal-charges/theft-overview.html (last visited Oct. 23, 2019).

[4] Stuart P. Green, *Introduction: Symposium on Thirteen Ways to Steal A Bicycle*, 47 NEW ENG. L. REV. 795, 796 (2013).

minimis, and the loss of the photos – perhaps the only copy of Larry's effort – to be the greater injury.[5]

> "By the mid-twentieth century, … theft reform became a primary goal of the American Law Institute, in drafting its Model Penal Code, first promulgated in 1962, while in England, theft reform became an early goal of the Criminal Law Revision Committee, the precursor to the Law Commission of England and Wales, which drafted what would become the Theft Act of 1968. Both efforts led to criminal codes that eliminated supposedly archaic distinctions such as those between larceny, embezzlement, and false pretenses, and replaced them with a more-or-less consolidated offense of 'theft.'"[6]

Does it matter whether Larry has a backup of the photos?[7] Does it matter that Larry has been deprived of the only copy, or is it that someone has, without Larry's permission, accessed his property without permission? We can readily see that a theft has occurred, not only of the flash drive, but also of the information which was contained on it. So, what happens if the information is taken *without* the theft of the thumb drive? "[I]s remote cyber bank theft more blameworthy than conventional bank theft? If cyber theft really is harder to detect or apprehend, would that fact by itself make the offender more culpable?"[8]

Consider Larry's photographic images being taken and used without payment for commercial purposes. Few would doubt that something has been taken, but the value he is owed as compensation is hard to determine. Can Larry's photos be recreated? Were they of an event that will never happen again? Are these commercial photos, or "just" personal photos of Larry and friends? If there is no other record of what was on the flash drive, is Larry limited in seeking only the replacement value of the physical drive, as opposed to the value of the intangible photos?

"I believe," [Prof. Brenner] says, that "my identity--my name-does have . . . value and should qualify for protection under the law of theft."[9] As support, she cites a passage from Shakespeare's Othello:

Who steals my purse steals trash; 'tis something, nothing; 'Twas mine, 'tis his, and has been slave to thousands. // But he that filches

---

[5] *See generally* Geraldine Szott Moohr, *Federal Criminal Fraud and the Development of Intangible Property Rights in Information*, 2000 U. ILL. L. REV. 683 (2000).

[6] Green, *supra* note 4, at 797.

[7] *See* Thomas G. Field, *Crimes Involving Intangible Property*, 11 U. N.H. L. REV. 171 (2013).

[8] Green, *supra* note 4, at 803.

[9] *Id.* at 804.

from me my good name // Robs me of that which not enriches him // And makes me poor indeed."[10]

C. Cyber Theft

Asportation, or "taking" is a salient element in traditional theft. However, cyber theft does not always involve a "taking" at all. This aspect often is far less meaningful to the victim of cyber theft than the interference with his or her property rights. As a result, meaningful remuneration sometimes escapes the victim if this element is not properly fulfilled.

The asportation element in cyber theft is well defined as carrying away a copy of someone else's data. The victim usually still has a copy of the data but is no longer has sole possession or access. What has been taken is the owner's sole possession or, in other words, her right of private access. [11]

Stealing the sole access or possession poses challenges for traditional notions of the definition of property, in the theft context. Theft remuneration and even gradation of the offense is based upon value of property stolen. The property stolen may be intangible, and the value may hinge on the possibility of dissemination of the data that devalues it commercially (in the case of Larry's professional photos) or invades the privacy of the owner (in the case of personal data). Each case is highly fact specific. The problem with "theft," in the digital/intangible/informational sense, is that we must struggle with the sense of the crime. Is it that the owner of property has been deprived of its use? Is it that the victim's ownership, or possession, or maybe even privacy and peace has been disturbed? Is it that access has been taken where it would not have been given?

> Theft and cyber theft are distinguished on the basis that theft is a zero-sum offense, in which sole possession of the property, such as funds, information, or software, is transferred from the rightful owner to the thief, while cybertheft is a non-zero-sum offense. The non-zero-sum offense consists of interfering with, rather than carrying away, the rightful owner's property with the intention to permanently, and wholly, deprive him or her of its possession and use. The dynamic usually involved in non-zero-sum theft consists of the cyber-thief's copying data that belongs to someone else and "carrying [the copy] away." This scenario

---

[10] *Id.* at 805 (quoting WILLIAM SHAKESPEARE, OTHELLO act 3, sc. 3, http://shakespeare.mit.edu/othello/othello.3.3.html).

[11] Susan W. Brenner*, Bits, Bytes, and Bicycles: Theft and "Cyber Theft"*, 47 NEW ENG. L. REV. 817, 821 (2016).

> does not involve a zero-sum offense because the victim retains possession of his or her property albeit in diminished capacity because the victim is no longer the sole possessor of the information. Unfortunately, while the dichotomy between theft (zero-sum transaction) and cybertheft (non-zero-sum transaction) can be absolute, it can also be more nuanced. The ambiguities that can creep in to the varieties of cyber theft are a function of the conceptual deficit that exists in this area.[12]

In order to align cyber*theft* with the notion of traditional theft, we would have to pigeonhole what the "thief" has stolen into the notion of property. While we can do that (with some mental and legal gymnastics![13]), it is not always pretty, nor is it always consistent.

But for us, the question is not limited to the notion of theft, because we are really looking at the question of *damage*. This is a much broader concept, because not only does it include damage from theft, but it also includes damage from tort.

These questions form an interesting background for breach litigation, but not a complete one. Most of the litigation does not involve the hacker/thief, who may not ever be found and who may not be operating in the same jurisdiction. What happens when the theft happens to a trusted third party? To answer this question, we need to discuss the law of torts.

II. THE LAW OF TORTS

A. Cyber Remedies in Tort.

Tort violations may result from intentional actions, a breach of duty as in negligence, or due to a violation of statutes.[14] Tort liability depends on the existence of a legal duty – for "where there is no duty there is no liability."[15]

In cases of cyber breaches, there are two common types of defendants: 1) a hacker or thief who intentionally caused harm, and 2) a third-party holding data that negligently breached a duty to safeguard personal information. The hacker-thief and his assets are unlikely to be served and attached. He may be in another country, known merely by an online moniker or even an IP address, making costs of bringing him to court impractical. As a result, many cases seek damages solely

---

[12] *Id.*

[13] See infra, Part V.B.

[14] *See Tort Law Liability*, LEGALMATCH, https://www.legalmatch.com/law-library/article/tort-law-liability.html (last visited Oct. 28, 2019).

[15] Bucheleres v. Chicago Park Dist., 171 Ill. 2d 435, 447 (Sup. Ct. 1996).

from the trusted third-party data holder, who is likely to be solvent and easy to serve.

The statutory right to privacy (in tort) may be breached by third party data holders when they negligently fail to safeguard personal data. However, many financial institutions are setting a higher standard than that of the statutory right to privacy. For example, the policy of one major banking institution, which is not atypical, states in reassuring terms:

> The law gives you certain privacy rights. Bank of America gives you more.
>
> . . . .
>
> Keeping financial information secure is one of our most important responsibilities. We maintain physical, electronic and procedural safeguards to protect Customer Information.
>
> . . . .
>
> . . . All companies that act on our behalf are contractually obligated to keep the information we provide to them confidential . . . .[16]

A customer reading this information would conclude, at a minimum, that in exchange for entrusting the bank with personal information, the bank agreed (1) to protect the data by means of physical, electronic, and procedural safeguards and (2) to keep it confidential. "Other language in the privacy policy reinforces those sensible conclusions by stressing the importance of precautions on the part of the customer to guard against disclosure or unauthorized use of account and personal information."[17]

B. Bailment as a Cause of Action for Cyber Violations

While bailment may seem an antiquated term when referring to intangible assets, the concept proves relevant when a trusted third-party fails to safeguard personal information. "A bailment relationship is said to arise where an owner, while retaining title, delivers personalty to another for some particular purpose upon an express or implied contract. The relationship includes a return of the goods to the owner or a subsequent disposition in accordance with his instructions." [18] Historically, the property may be tangible or intangible.[19]

---

[16] Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, n. 152 (2005).

[17] *Id.* at 279.

[18] Lionberger v. United States, 371 F.2d 831, 840 (Ct. Cl. 1967).

[19] *See, e.g.*, Liddle v. Salem Sch. Dist. No. 600, 249 Ill. App. 3d 768 (1993) (information in a letter was property that could be the subject of a bailment).

That property can include money,[20] choses in action,[21] negotiable notes, bonds, corporate stock, insurance policies, and checks.[22] It can also include client lists,[23] digital music files,[24] and data and software.[25]

The requirement that the property be returned has been overemphasized, as a disposition or destruction will suffice.

> A 'bailment' in its ordinary legal sense imports the delivery of personal property by the bailor to the bailee who keeps the property in trust for a specific purpose, with a contract, express or implied, that the trust shall be faithfully executed, and the property returned *or duly accounted for* when the special purpose is accomplished or that the property shall be kept until the bailor reclaims it.[26]

Breach of the trust created by a bailment results in liability of the bailee for conversion. "Any unauthorized delivery of bailed property by a bailee—even delivery to the wrong person resulting from the bailee's good faith mistake—constitutes a conversion."[27] Further, "bailees are 'not only liable for losses occasioned by their negligence, but for those which arise from innocent mistakes in the delivery of goods to persons not entitled to receive them."[28]

However, not every court agrees that personal identifying information is property.[29] To be fair, there is a good argument that *some* information is not property, because it is not *sensitive* or *private* or *unique* enough.[30] There are a few reasons why, at least in the context

---

[20] In re LGI Energy Solutions, Inc., 460 B.R. 720, 728 (B.A.P. 8th Cir. 2011).

[21] Van Wagoner v. Buckley, 148 A.D. 808 (N.Y. App. Div. 1912).

[22] Dean Witter Reynolds, Inc. v. Variable Annuity Life Ins. Co., 373 F.3d 1100, 1107 (10th Cir. 2004).

[23] *See, e.g.*, Shmueli v. Corcoran Group, 9 Misc. 3d 589 (Sup. Ct. 2005).

[24] Marchello v. Perfect Little Prods., Inc., 94 A.D.3d 825 (Sup. Ct. 2012).

[25] David Barr Realtors, Inc. v. Sadei, No. 03-97-00138-CV, 1998 WL 333954 (Tex. Ct. App. 1998).

[26] Weinberg v. Wayco Petroleum Co., 402 S.W.2d 597, 599 (Mo. App. 1966).

[27] Fireman's Fund Ins. Co. v. Wagner Fur, Inc., 760 F.Supp. 1101, 1105 (S.D.N.Y.1991) (emphasis in original) (citing RESTATEMENT (SECOND) OF TORTS § 234 and § 234 cmt. a.).

[28] Dean Witter Reynolds Inc. v. Variable Annuity Life Ins. Co., 373 F.3d 1100, 1106 (10th Cir. 2004) (internal citations omitted).

[29] Enslin v. Coca-Cola Co., 136 F. Supp. 3d 654, 679 (E.D. Pa. 2015), *aff'd sub nom*. Enslin v. Coca-Cola Co., 739 Fed. Appx. 91 (3d Cir. 2018); Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008) (social security numbers and credit card information stolen from a computer were not property for purposes of the law of bailment); In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 974-75 ("the Court is 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.") In re Target Corp. Customer Data Sec. Breach of Litig., 66 F. Supp. 3d 1154, 1177.

[30] Ree v. Zappos.com, Inc., 888 F.3d 1020, 1026 (9th Cir. 2018), *cert. denied sub nom*. Zappos.com, Inc. v. Stevens, 139 S.Ct. 1373 (2019) (Congress recognized that credit card

of breach litigation, that this argument is flawed. First, the fact that some hacker found value in the information speaks to the fact that information can be treated as property. Recognizing the fact that the hacker will package the information and then *sell* it to others leaves us begging the question … did the hacker have property? Was it stolen?

Second, the whole concept of *identity theft* recognizes, at least on some level, that a person's identity can be a protectable, legally-cognizable right.[31] And finally, entire industries exist because "data is power."[32] Google, Facebook and numerous others have built empires based on this market reality. Furthermore, when one company exchanges information for consideration with another company, what do you call the information but property?

This mental exercise just leads us back to the original question: Has the victim, who entrusted her PII to a store, suffered harm when that information is taken? Is the store liable? Is this a matter of trust (both in the colloquial sense as well as the legal sense)?

C. Conversion

Once a bailee has received property from another, they have a duty to return or account for the property. But what standard do we apply to ascertain a breach of that duty? Ordinary negligence? Gross negligence? Is the bailee a fiduciary?[33]

If we find conversion, what is the measure of damages? We can't reseal Pandora's Box, or restore privacy, although courts and legislatures would love to try.[34]

III. OTHER BASES FOR LIABILITY

A. Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681, enacted to promote the "confidentiality, accuracy, relevancy, and proper utilization"[35] of consumer information reported by consumer reporting

---

information was sensitive).

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

[32] Frederike Kaltheuner & Elettra Bietti, *Data is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR*, 2 J. INFO. RIGHTS POL'Y & PRAC. (2017), https://journals.winchesteruniversitypress.org/index.php/jirpp/article/view/45 [https://perma.cc/8YMX-EYLS].

[33] *See* Richard. H. Helmholz, *Bailment Theories and the Liability of Bailees: The Elusive Uniform Standard of Reasonable Care*, 41 U. OF KAN. L. REV.97 (1992).

[34] *See* Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (May 13, 2014), http://perma.cc/ED5L-DZRK; Council Regulation 2016/679, art. 17, 2016 O.J. (119) 1, https://gdpr-info.eu/art-17-gdpr/.

[35] 15 U.S.C. § 1681(b).

agencies. It was intended to protect consumers from the willful and/or negligent inclusion of inaccurate information in their credit reports.[36]

The FCRA requires that any "consumer reporting agency" – which includes organizations that "regularly…assembl[e] or evaluat[e] consumer credit information . . . for the purpose of furnishing consumer reports to third parties"[37] – that "fails to comply with any requirement imposed under [the FCRA] with respect to any consumer is liable to that consumer…". [38]

However, the FCRA is old. It was enacted in 1970 and was not designed as a remedy or enabling legislation for modern data breaches. Plaintiffs looking for federal jurisdiction through the FCRA find it difficult to shoehorn their claims into the FCRA's language of "furnishing consumer reports."[39]

As will be discussed below, when looking at Article III standing, the Third Circuit has considered the violation of the FCRA alone to be sufficient injury for standing to exist.[40]

B. State Law Claims

A number of data breach causes of action are found in state law, including claims for negligence, breach of implied contract, invasion of privacy and unjust enrichment.[41] These claims do not grant federal jurisdiction, and are limited to the plaintiffs who reside in that state.

All fifty states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have legislation requiring private or governmental entities to disclose security breaches involving PII.[42] Not all of these

---

[36] "Liability for negligent violations of the FCRA is created by 15 U.S.C. § 1681o. Liability for willful violations is created by 15 U.S.C. § 1681n, which also provides for punitive damages upon a finding of willful noncompliance." Krajewski v. Am. Honda Fin. Corp., 557 F. Supp. 2d 596, 613 (E.D. Pa. 2008).

[37] 15 U.S.C. § 1681a(f); see also 16 CFR Part 681.1.

[38] 15 U.S.C. § 1681n.

[39] *See, e.g.*, Holmes v. Countrywide Financial Corp., No. 5:08-CV-00205-R, 2012 WL 2873892, at *15 (D. W.D. Ky. July 12, 2012).

[40] *See infra* VI.C.3.a.

[41] *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 663 Fed. Appx. 384, 386 (6th Cir. 2016); *see also* Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012).

[42] *Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Sept. 29, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

grant a private right of action to victims,[43] but some do,[44] and some courts and executive officers are reading in private rights.[45]

The difficulty is that, both for companies who process PII and for their customers, it creates a patchwork of legislation, regulation, and compliance regimes. Even small companies (and, for that matter, nonprofits, hospitals, schools, etc.) find themselves doing business with individuals and entities in more than one state. The cost of compliance with data protection regulations continues to rise.[46]

C. International Regimes

A very small number of international data protection regimes purport to give victims of data breaches a private right of action.[47] GDPR Article 82(1) provides, "[a]ny person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."[48] And Article 80(2) provides that "the data subject shall have the right to mandate a not-for-profit body, organisation or association … to lodge the complaint on his or her behalf."[49] The world continues to struggle with how to handle data protection.

---

[43] *See, e.g.*, S.B. 318, Act No. 396 (Ala. 2018).

[44] *See generally Data Breach Charts*, BAKERHOSTETLER 26-27 (July 2018), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf; California Consumer Privacy Act of 2018.

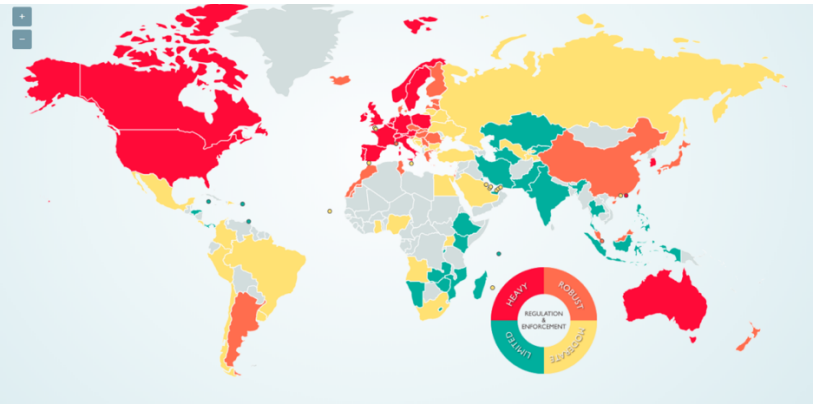
[45] Rosenbach v. Six Flags Entertainment Corporation, 2019 IL 123186, ¶ 40 (Sup. Ct. 2019) ("an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act.").

[46] The "average cost of compliance for the organizations in our current study is $5.47 million, a 43 percent increase from 2011 . . . ." PONEMON INST. LLC, THE TRUE COST OF COMPLIANCE WITH DATA PROTECTION REGULATIONS 4 (Dec. 2017), https://dynamic.globalscape.com/files/Whitepaper-The-True-Cost-of-Compliance-with-Data-Protection-Regulations.pdf.

[47] *See, e.g.,* Natasha G. Kohne, Mazen Baddar & Diana E. Schaffner, *Bahrain's Personal Data Protection Law Now in Force*, AKIN GUMP (Aug. 20, 2019), https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/bahrain-s-new-data-protection-law-now-in-force.html; Privacy Bill 2018, s 103 (N.Z.).; The Personal Data Protection Bill (Draft), 2018, s 75 (India), https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf; Civil Code (promulgated by Ministry of Justice, 2019) FAWUBU FAGUI ZILIAOKU, art. 195 (Taiwan), https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=B0000001.

[48] *See generally* General Data Protection Regulation (GDPR), art. 82(1), May 25, 2018, *available at* https://gdpr-info.eu/art-82-gdpr/.

[49] John Patzakis, Esq. & Craig Carpenter, *GDPR Provides a Private Right of Action. Here's Why That's Important*, X1 EDISCOVERY L. & TECH BLOG (Feb. 28, 2018, 8:51 AM), https://blog.x1discovery.com/2018/02/28/gdpr-provides-a-private-right-of-action-heres-why-thats-important/.



The above image shows nations of the world who have enacted some form of data protection legislation with their relative levels of complexity.[50]

IV. THE NATURE OF PERSONAL INFORMATION

The idea of being harmed by the disclosure of personal information depends on an understanding of what is *personal information*, which in turn forces us to ask what is private? If the information is not private, then there should be no harm in its dissemination, whether lawful or not.

A. PII in the United States

The United States uses the concept of PII. The National Institute of Standards and Technology ("NIST")[51] provides the following definition of PII:

> PII is any information about an individual … including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[52]

---

[50] *Data Protection Laws of the* World, DLA PIPER, https://www.dlapiperdataprotection.com/ (last visited Oct. 29, 2019).

[51] NATI'L INST. OF STANDARDS AND TECH., http://www.nist.gov/ (last visited Oct. 29, 2019).

[52] ERIKA MCCALLISTER, TIM GRANCE, & KAREN SCARFONE, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) ES-1 (Nat'l Inst. of Standards and Tech, Apr. 2019) (also known as NIST Special Publication 800-122), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf; *Glossary*, COMPUTER SECURITY RESOURCE CTR., https://csrc.nist.gov/glossary/term/personally-identifiable-information (last visited Oct. 30, 2019).; *see also Rules and Policies – Protecting*

Why is this important? Because we recognize that not all information is equally private. The NIST definition includes a distinction between linked and linkable information, the difference being information that is uniquely yours (i.e. can be used to identify you)[53] and information which, when combined with other information, could be used to identify you.[54]

That "any other information" prong is problematic, because it makes the definition of PII fluid. In a post following a 2016 speech in San Francisco, Jessica Rich, the Director of Bureau of Consumer Protection from the Federal Trade Commission (FTC), mentioned the topic of linkable information:

> We [the FTC] regard data as 'personally identifiable,' and thus warranting privacy protections, when it can be *reasonably linked* to a particular person, computer, or device. In many cases, persistent identifiers such as device identifiers, MAC addresses, static IP addresses, or cookies meet this test. [55]

Note the expansion of PII to include the identification, not only of a person, but of a computer or device.

The combination of a name with other information, for example, a name on a list of patients for an abortion clinic, can be PII. However, bits of information, taken alone, can still be PII if they can later be combined with other information to identify persons.

It may also be helpful to note that many states have enacted their own data protection laws with PII-like definitions. Consider the California Consumer Privacy Act of 2018:

"'Personal information' means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[56]

Under the Act, personal information includes

- names, aliases, postal addresses, unique personal identifiers, online identifier Internet Protocol address, email address, account

---

PII – Privacy Act, U.S. GEN. SERV. ADMIN., https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act (last visited Oct. 30, 2019).

[53] Examples include an email address, social security number, passport number, driver's license number, and credit card number.

[54] Examples also include a common last names, date of birth, race, gender, and age.

[55] Jessica Rich, *Keeping Up with the Online Advertising Industry*, FED. TRADE COMMISSION (Apr. 21, 2016, 10:30 AM), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry (emphasis in original).

[56] Cal. Civ. Code § 1798.140(o)(1), http://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375.

name, social security number, driver's license number, passport number, or other similar identifiers.

- records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

- biometric information.

- internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

- geolocation data.

- audio, electronic, visual, thermal, olfactory, or similar information.

- professional, employment-related or education information.

- inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.[57]

B. Personal Information in the EU

The EU's General Data Protection Regulation ("GDPR") defines Personal data as the following:

> For the purposes of this Regulation:
> (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[58]

Recital 30 expands on this. "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers

---

[57] *Id.* at § 1798.140(o)(1)(A)-(K).

[58] Council Regulation 2016/679, art. 4, 2016 O.J. (119) 1, http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm.

and other information received by the servers, may be used to create profiles of the natural persons and identify them."[59]

The GDPR took effect in May of 2018, and there are many questions yet unanswered about its scope and effect. However, at least initially, we can note that the GDPR's definition is broader, in that it attempts to include direct *or indirect* identification and does not require the information to identify the person, but that the person could be "identifiable."

C. Personal Information in China

China's Personal Information Security Specification took effect in May 2018. The Specification is the "effective centerpiece of an emerging system around personal data," which includes the 2017 Cybersecurity Law.[60] The CSL loosely defines both personal data and a new category of personal sensitive data, which may include "data that may lead to bodily harm, property damage, reputational harm, harm to personal heath, or discriminative treatment of an individual if such data is disclosed, leaked or abused."[61]

V. DAMAGES

A. The Case or Controversy Clause and Cyber Theft

When no financial harm has been experienced yet by the victims of cyber theft of data, the circuit courts are split as to whether a case or controversy exists.

> Article III, Section 2, Clause 1 of the Constitution states:
> The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority;—to all Cases affecting Ambassadors, other public ministers and Consuls;—to all Cases of admiralty and maritime Jurisdiction;—to Controversies to which the United States shall be a Party;—to Controversies between two or more States;—between a State and Citizens of another State;—between Citizens of different States;—between Citizens of the same State claiming Lands under Grants of different States, and

---

[59] Council Regulation 2016/679, Recital 30, 2016 O.K. (119) 1, http://www.privacy-regulation.eu/en/r30.htm.

[60] Mingli Shi, Samm Sacks, Qiheng Chen, & Graham Webster, *Translation: China's Personal Information Security Specification*, NEW AMERICA (Feb. 8, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/.

[61] *Id.*

> between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.[62]

"[S]etting apart the 'Cases' and 'Controversies' that are of the justiciable sort referred to in Article III—'serv[ing] to identify those disputes which are appropriately resolved through the judicial process,'—is the doctrine of standing."[63]

The Supreme Court has established three elements of Article III standing:

1) an injury in fact that is concrete and particularized;
2) a causal connection between the conduct and the resulting injury; and
3) a likelihood that the injury will be redressable by the court.[64]

In breach cases, Article III standing usually comes into play with respect to elements 1 and 2.

With respect to the "concreteness" element, defendants have argued that although they admit a breach, plaintiffs were not harmed. This happens because at the time of the litigation, very few plaintiffs may be able to show financial injury. There may be personal information exposed, but how many fraudulent credit transactions or identity theft cases follow? And, at least in a few of the cases, the bank or the defendant offers to cover the cost of the fraud, thus the plaintiff is made whole – at least in one financial sense.

With regard to the causal element, defendants have argued that plaintiffs have not proven that their action – allowing a breach to occur or failing to protect customer data – is the cause of the plaintiffs' injury. The Supreme Court has recognized that this element can lead to a very attenuated, speculative chain of events, and has held that no standing exists in these instances.[65]

One major difficulty all these cases demonstrate is that the data thief is not in court. The plaintiff has suffered an injury at the hacker's hand, but the data is being held by a third party. While the state of cyberlaw is changing, plaintiffs and lawmakers struggle with the question of whether to hold data processors liable, for how much, and to whom? Besides the public shock at having trust eroded, and the violation of identity theft, is it appropriate, *under Article III*, to hold a business accountable to all the public? Whose records were taken? Whose records were misused (and is that even a concern)?

---

[62] U.S. Const. art. III, § 2, cl. 2.

[63] Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).

[64] *Id.* at 560-61.

[65] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).

At the beginning of the article, we asked about stolen bicycles. Theft of a tangible item deprives the user of all enjoyment and use. Does "theft" accurately describe misappropriation of data?

Conversion or trespass is understandable with tangible property, but does it accurately describe the relationship between the plaintiff and the defendant store, hospital, or insurance company? A bailee is liable if she cannot account for the property entrusted to her care, but is personal information bailable property? Does the mere violation of a statute create a cognizable injury for standing purposes?

These are the questions confronting the courts, who have been facing a growing number of breaches and a growing number of class action filings. The circuit courts of appeal have split on the issue of whether, at the pleading stage, Article III standing has been adequately plead if no financial harm can be shown to exist … yet.

B. Circuit Court Split

1. CareFirst

> The Court's denial of certiorari is clearly good news for the Plaintiffs, and may signal that the Supreme Court, at least as of now, is comfortable with the ongoing split among courts of appeal over the viability of data breach class actions in federal court. The Sixth, Seventh, Ninth, and D.C Circuits have permitted data breach class actions to proceed based on a fear of identity theft, whereas the First, Third and Fourth have not. (The Third Circuit, however, has allowed a data breach class action to proceed based on violation of the FCRA's confidentiality requirements.) There is a modest trend among Courts of Appeal that have recently addressed the issue to find that standing exists in data breach class actions where the breach was caused by cybercriminals.[66]

What did the Appeals Court in Attias v. CareFirst think was the injury?

After discussing cases which analyzed Article III standing based on risk of future injury, the court made this statement: "Under our precedent, 'the proper way to analyze an increased-risk-of-harm claim is to consider the ultimate alleged harm,' which in this case would be identity theft, 'as the concrete and particularized injury and then to

---

[66] Phillip N. Yannella & Edward J. McAndrew, *Supreme Court Denies Cert Petition in Carefirst v. Attias*, THE NAT'L L. REV. (Feb. 21, 2018), https://www.natlawreview.com/article/supreme-court-denies-cert-petition-carefirst-v-attias.

determine whether the increased risk of such harm makes injury to an individual citizen sufficiently 'imminent' for standing purposes.'"[67]

But what did the court think identify theft was? "Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury. The remaining question, then, keeping in mind the light burden of proof the plaintiffs bear at the pleading stage, is whether the complaint plausibly alleges that the plaintiffs now face a substantial risk of identity theft as a result of CareFirst's alleged negligence in the data breach."[68]

The court then went on the analyze the district court's dismissal of the complaint "because they [plaintiffs] had 'not suggested, let alone demonstrated, how the CareFirst hackers could steal their identities without access to their social security or credit card numbers….'"[69]

Here's a flaw in the argument. Is the harm suffered by the plaintiffs limited to the potential to have their identities stolen? Or has the harm already occurred, because PII stored by a trusted source been exposed to outsiders?

"So we have specific allegations in the complaint that CareFirst collected and stored "PII/PHI/Sensitive Information," a category of information that includes credit card and social security numbers; that PII, PHI, and sensitive information were stolen in the breach; and that the data "accessed on Defendants' servers" place plaintiffs at a high risk of financial fraud. The complaint thus plausibly alleges that the CareFirst data breach exposed customers' social security and credit card numbers. CareFirst does not seriously dispute that plaintiffs would face a substantial risk of identity theft if their social security and credit card numbers were accessed by a network intruder, and, drawing on "experience and common sense," we agree."[70]

We can see the court struggling with the right answer but approaching it from the wrong starting point. This is understandable, if we consider that the only harm is to have someone masquerade as you and obtain financial gain fraudulently.

But if we return to my stolen bicycle, the harm occurs not when someone else decides to ride it (although conceptually we could then put a "lost opportunity cost" dollar figure to that), but when someone

---

[67] Attias v. Carefirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017), *cert. denied*, 138 S.Ct. 981 (2018) (citing Food & Water Watch, 808 F.3d at 915 (quoting Public Citizen, Inc. v. Nat'l Highway Traffic Safety Admin., 489 F.3d 1279, 1298 (D.C. Cir. 2007)).

[68] *Id.*

[69] *Id.*

[70] *Id.* at 628.

takes the bike out of my garage. The harm is that I've been deprived of the bike, and not necessarily that someone else is using it.

Does that analogy translate directly to PII? Part of the problem the Court is struggling with is the nature of digital information. Unlike the bike, it can be copied multiple times, and the original (if such a concept exists!) is not diminished by the use of the copies. But is that the true nature of the injury?

2. Privacy Redux

In 1890, two young Boston attorneys wrote an essay for the Harvard Law Review entitled, "The Right to Privacy."[71] In it they argued that the law protects the privacy of individuals against wrongful intrusion. "We must therefore conclude that the rights, so protected, whatever their exact nature, are not rights arising from contract or from special trust, but are rights as against the world; and, as above state, the principle which has been applied to protect these rights is in reality not the principle of private property [which may be the subject of identity theft, for example] …. The principle which protects personal writings *and any other productions of the intellect or of the emotions*, is the right to privacy …."[72]

Looking to theft for protection from a breach focuses on the nature of PII as property. It may indeed be property *in the hands of the third-party possessor*, but that inquiry focuses on the website or business that has collected the information of another. For them, theft of property may be the right legal issue.[73] The more relevant inquiry for the individual whose information is should be: has their privacy been invaded? Has wrongful intrusion occurred?

Notice that if the answer to those questions is "yes", then we have satisfied the injury in fact question rather neatly. We do not need to entertain the question raised by many courts of whether the injury is speculative or lies in the future, for an injury to privacy occurs upon the instant when there is intrusion upon another's privacy.

---

[71] Warren & Brandeis, *supra* note 31, at 193.

[72] *Id.*

[73] *But see* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 968 (7th Cir. 2016) ("Plaintiffs also claim that they have a property right to their personally identifiable data, and that the theft of their data supports standing just as well as the theft of one's car would. But the only authority to which they direct us is Sterk v. Redbox Automated Retail, LLC, 770 F.3d 618 (7th Cir.2014), which says nothing of the kind.").

3. Courts That Found Standing

a. Third Circuit

In *In re: Horizon Healthcare Services Inc. Data Breach Litigation*, the court recognized that "In the context of a motion to dismiss, we have held that the [i]njury-in-fact element is not Mount Everest. The contours of the injury-in-fact requirement, while not precisely defined, are very generous, requiring only that claimant allege[ ] some specific, identifiable trifle of injury."[74]

In fact, the Third Circuit seems to be the most generous in terms of allowing standing.

In November of 2013, two laptop computers containing unencrypted personal information of more than 839,000 customers were stolen from Horizon's headquarters.[75] After discovering the theft, Horizon notified law enforcement immediately, and then alerted customers by letter and a press release a month later, on December 6, stating that there were differing amounts of PII that may have been exposed.[76] Some, but not all of the plaintiffs suffered direct financial harm (including one plaintiff who had a fraudulent tax return filed in his name).[77]

The trial court dismissed the complaint, concluding "that standing requires some form of additional, "specific harm," beyond "mere violations of statutory and common law rights[.]""[78] Although the court was convinced that at least one of the plaintiffs had suffered a harm that would meet any of the Article III standards we have previously discussed, the court proceeded to address the issue of whether a violation of a statute can give rise to Article III standing without additional concrete financial harm.[79] The court agreed that it could citing several Supreme Court cases as precedent.[80]

---

[74] In re Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 633 (3d Cir. 2017) (quoting Blunt v. Lower Merion Sch. Dist., 767 F.3d 247, 278 (3d Cir. 2014)).
[75] *Id.* at 630.
[76] *Id.*
[77] *Id.*
[78] *Id.* at 634.
[79] *Id.* at 635.
[80] *See* Warth v. Seldin, 422 U.S. 490, 500 (1975) ("The actual or threatened injury required by Art[icle] III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing." (citation, internal quotation marks, and ellipses omitted)); Linda R.S. v. Richard D., 410 U.S. 614, 617 n.3 (1973) ("Congress may enact statutes creating legal rights, the invasion of which creates standing, even though no injury would exist without the statute.").

Next, the Court looked at its own history of Article III litigation, and noted that it had not been consistent.[81] But the court pointed to two recent cases, *In re Google*[82] and *In re Nickelodeon*,[83] for the propositions that:

- so long as an injury "affect[s] the plaintiff in a personal and individual way," the plaintiff need not "suffer any particular type of harm to have standing."[84]
- "the actual or threatened injury required by Art[icle] III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing," even absent evidence of actual monetary loss;[85] and
- "when it comes to laws that protect privacy, a focus on economic loss is misplaced" and "the unlawful disclosure of legally protected information" is "a clear de facto injury."[86]

The court then turned to *Spokeo*.[87] "Although it is possible to read the Supreme Court's decision in *Spokeo* as creating a requirement that a plaintiff show a statutory violation has caused a "material risk of harm" before he can bring suit,"[88] the court noted that the Supreme Court "rejected the argument that an injury must be "tangible" in order to be "concrete.""[89] Instead, *Spokeo* teaches that Congress "has the power to define injuries,"[90] including intangible injuries that give rise to Article III standing. However, "there are some circumstances where the mere technical violation of a procedural requirement of a statute cannot, in and of itself, constitute an injury in fact."[91]

Judge Schwartz, concurring, decided that the theft of the laptop showed invasion of privacy, and therefore, no additional analysis was needed to show a concrete injury.[92]

---

[81] *In re Horizon*, 846 F.3d at 635.

[82] In re Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125 (3d Cir. 2015).

[83] In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262 (3d Cir. 2016).

[84] *In re Google Inc.*, 806 F.3d at 134.

[85] *Id.*

[86] *In re Nickelodeon*, 827 F.3d at 272-274.

[87] *Spokeo, Inc.*, 136 S.Ct. at 1540.

[88] Noting that the Eighth Circuit had read the case in just that way. *In re Horizon*, 846 F.3d at 637.

[89] *Spokeo, Inc.*, 136 S.Ct. at 1549.

[90] *Id.*

[91] *In re Horizon*, 846 F.3d at 638.

[92] *Id.* at 641.

b. Sixth Circuit

In *Galaria v. Nationwide*,[93] plaintiffs brought putative class actions after hackers breached the computer network of Nationwide Mutual Insurance Company. Plaintiffs alleged invasion of privacy, negligence, and violations of the Fair Credit Reporting Act (FCRA).[94] The district court dismissed the complaints, concluding that plaintiffs had failed to state a claim for invasion of privacy, lacked Article III standing to bring the negligence claims, and lacked statutory standing to bring the FCRA claims.[95]

On appeal, the Sixth Circuit reversed, finding that the plaintiffs had Article III standing and that the district court erred in dismissing the FCRA claims. With respect to Article III standing, the Court proceeded with the *Spokeo*[96] three element test for standing: (1) There must be an injury, (2) it must be fairly traceable to the conduct being challenged, and (3) the injury will likely be redressed by a favorable decision.[97]

With respect to the first prong, the court explained that an injury must be actual or imminent, and then decided to follow the other courts that have dealt with this issue by assuming that data theft occurs in two phases --- the lifting of the data, and then the misuse of the data.[98] I will explain later why this is an incorrect way of looking at data breach damages, but here the Court reaches the right result. "Here, Plaintiffs' allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage of the litigation."[99] In fact, the court *almost* gets it right.

> There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals….Thus, although it might not be 'literally certain' that Plaintiffs' data will be misused, there is a sufficiently substantial risk of harm that incurring mitigation costs is reasonable. Where Plaintiffs already know that they have lost control of their data, it would be unreasonable to expect Plaintiffs to wait for actual misuse—a fraudulent charge on a credit card, for example—before taking steps to ensure

[93] Galaria v. Nationwide Mutual Ins. Co., 663 F. App'x 384, 385–86 (6th Cir. 2016).
[94] *Id.*
[95] *Id.* at 387.
[96] Injury is "the '[f]irst and foremost' of standing's three elements." *Galaria*, 663 F. App'x at 388 (citing *Spokeo*, 136 S.Ct. at 1547).
[97] *Lujan*, 504 U.S. at 560–61.
[98] *Galaria*, 663 F. App'x at 388-89.
[99] *Id.* at 388.

> their own personal and financial security, particularly when Nationwide recommended taking these steps.[100]

As we can see, the Court was more persuaded that plaintiffs' mitigation costs, coupled with Nationwide's offer of credit monitoring, was enough to show injury. Left for another day was the issue of whether the theft itself was injury enough.

The majority had no issues with the other two prongs of the test, but the dissent was bothered that the second factor of traceability was not met.

> The complaints simply allege that hackers were in fact able to access the plaintiffs' personal information. From that fact, the complaints conclude that Nationwide failed to protect that information. But plaintiffs make no factual allegations regarding how the hackers were able to breach Nationwide's system, nor do they indicate what Nationwide might have done to prevent that breach but failed to do.[101]

This may have been both a pleading issue and a fundamental misunderstanding that the plaintiff has some duty to show *how* a breach occurred. This is not the case in other areas of the law. For example, in bailment, "a bailor need prove only (1) the contract of bailment, (2) delivery of the bailed property to the bailee and (3) failure of the bailee to redeliver the bailed property undamaged at the termination of the bailment."[102] It is not the bailor's duty to plead how the property was lost or damaged. Why should it be so with data?

c. Seventh Circuit

In 2013, hackers stole approximately 350,000 credit card numbers of Neiman Marcus customers.[103] The company learned of the breach in mid-December but kept the information confidential at first.[104] Neiman Marcus discovered potential malware in its computer systems on January 1, 2014 but waited until January 10, 2014 to announce the breach to the public, at which point several customers sued pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d).[105] The district court granted Neiman Marcus' motion to dismiss the complaint for lack of standing and for failure to state a claim.[106]

---

[100] *Id.*

[101] *Id.* at 392.

[102] David v. Lose, 218 N.E.2d 442 (Ohio 1966).

[103] Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 690 (7th Cir. 2015).

[104] *Id.*

[105] *Id.*

[106] *Id.* at 691.

d. Ninth Circuit

In *Zappos*,[107] more than 24 million customers had their "names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information"[108] taken by hackers. In the resulting class action litigation, "some of the plaintiffs alleged that the hackers used stolen information about them to conduct subsequent financial transactions" while some did not.[109] The appeal to the Ninth Circuit was based on the latter claims and focused on the hacking incident itself (not any subsequent illegal activity).

This is the second data breach case alleging problems with standing to appear before the Ninth Circuit. The court considered whether the prior case, *Krottner v. Starbucks Corp.*,[110] was still good law after the Supreme Court decision in *Clapper v. Amnesty International USA*.[111] The court concluded that it was,[112] and that *Krottner* and *Clapper* were reconcilable. First, the court recognized that the "injury in *Krottner* did not require a speculative multi-link chain of inferences. The *Krottner* laptop thief had all the information he needed to open accounts or spend money in the plaintiffs' names—actions that *Krottner* collectively treats as 'identity theft.'"[113] Second, the type of theft is important. *Krottner* involved the theft of PII on a laptop, while *Clapper* involved surveillance procedures authorized by the Foreign Intelligence Surveillance Act of 1978.[114] *Clapper* involved questions of national security and separation of powers,[115] which did not arise in *Krottner*. Third, the focus in *Clapper* was on the impending nature of the alleged injury, but the court noted that other cases have correctly focused on whether there is a "substantial risk" of injury (and not necessarily just an "impending" risk".[116]

Having decided that *Krottner* would control in the case, the court noted that this case also involved the theft of credit card numbers (which were not stolen in *Krottner*), and that Congress had recognized that credit card numbers are "sufficiently sensitive to warrant

---

[107] In re Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018), *cert. denied sub nom*. Zappos.com, Inc. v. Stevens, 139 S.Ct. 1373 (2019).
[108] *Id.*
[109] *Id.*
[110] 628 F.3d 1139, 1142–43 (9th Cir. 2010).
[111] 568 U.S. 398 (2013).
[112] *In re Zappos*, 888 F.3d at 1023.
[113] *Id.* at 1026.
[114] Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).
[115] *Clapper*, 568 U.S. at 398 (2013).
[116] *In re Zappos*, 888 F.3d at 1026.

legislation prohibiting merchants from printing such numbers on receipts."[117]

Zappos countered by arguing that even if the information which was taken was sensitive, finding standing is not appropriate because too much time had passed (the breach occurred in 2012, and the case was argued in 2018), and therefore, the alleged harm was speculative.[118] The court noted that argument might be appropriate later, but not for the motion to dismiss stage.[119] "Plaintiffs also specifically allege that '[a] person whose PII has been obtained and compromised may not see the full extent of identity theft or identity fraud for years.'"[120]

e. Eleventh Circuit

In *Resnick v. AvMed, Inc.*,[121] the defendant had two laptops taken from their corporate office in Gainesville, Florida in December of 2009. The laptops contained customers' sensitive information, including protected health information, Social Security numbers, names, addresses, and phone numbers.[122] AvMed did not encrypt the data, and the laptops were sold to a fence, along with PII from approximately 1.2 million current and former AvMed members.[123]

The court spent some time going through each of the plaintiffs' claims, but in the end, did not have a difficult time, since the named parties had both been victims of identity theft, and had suffered financial harm. The court (and the dissent) spent more time looking at the issue of causation.[124]

4. Courts That Denied Standing

a. First Circuit

In *Katz v. Pershing, LLC*,[125] the plaintiff had a brokerage account with a company that used the defendant's software service to "make its clients' nonpublic personal information, including social security numbers and taxpayer identification numbers, accessible to certain

---

[117] *Id.*
[118] *Id.* at 1028-29.
[119] *Id.*
[120] *Id.*
[121] 693 F.3d 1317 (11th Cir. 2012).
[122] *Id.* at 1322.
[123] *Id.*
[124] *Id.*
[125] 672 F.3d 64, 80 (1st Cir. 2012).

authorized end-users…."[126] The court struggled with the concept of standing. The plaintiff had privacy and identity theft concerns, and had even purchased identity monitoring services, but had no financial harm due to actual identity theft.[127]

The complaint alleged several state law claims, but the court still found no actual injury.

> [T]he plaintiff has not alleged that her nonpublic personal information actually has been accessed by any unauthorized person. Her cause of action rests entirely on the hypothesis that at some point an unauthorized, as-yet unidentified, third party might access her data and then attempt to purloin her identity. The conjectural nature of this hypothesis renders the plaintiff's case readily distinguishable from cases in which confidential data actually has been accessed through a security breach and persons involved in that breach have acted on the ill-gotten information.[128]

b. Second Circuit

In *Whalen v. Michaels Stores, Inc.*, the plaintiff used her card at Michaels Stores, and, following a breach of Michaels' network, discovered that her card was used twice in locations in Ecuador.[129] She prompted cancelled her card, and her bank took care of the fraudulent charge attempts.[130] The Second Circuit agreed with the district court that she lacked Article III standing, noting that she did not have any actual monetary damage with respect to the fraudulent charges, nor would she in the future, since the card was cancelled and no other PII was taken.[131] The court further remarked that she did not plead how she was financially harmed by having to spend time dealing with the fraudulent charges.[132]

---

[126] *Id.* at 69–70.
[127] *Id.* at 79.
[128] *Id.* at 79–80.
[129] Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017).
[130] *Id.*
[131] Additionally, she does not allege how she can plausibly face a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other personally identifying information—such as her birth date or Social Security number—is alleged to have been stolen. *Id.*
[132] *Cf. P.F. Chang's*, 819 F.3d at 967 ("P.F. Chang's accepts Remijas's holding that the time and money spent resolving fraudulent charges are cognizable injuries for Article III standing.").

c. Fourth Circuit

In *Beck v. McDonald*,[133] veterans who received medical treatment and health care at the Veterans Affairs Medical Center in Columbia, South Carolina sued after the theft of a laptop compromised their personal information. In February of 2013, a laptop went missing from the Center.[134] "The laptop contain[ed] unencrypted personal information of approximately 7,400 patients, including names, birth dates, the last four digits of social security numbers, and physical descriptors (age, race, gender, height, and weight)."[135]

An internal investigation was conducted and concluded that the laptop was likely stolen and that the Center failed to follow the policies for storing patient information.[136] The Center notified every affected patient and offered one year of free credit monitoring. The laptop was never recovered.[137]

Notice that the pleading in *Beck* was limited, listing only the "threat of current and future substantial harm from identity theft and other misuse of [Plaintiffs'] Personal Information."[138] The plaintiffs sought relief under the Privacy Act, the APA, and common law negligence.[139]

The district court initially dismissed the negligence claims, and after extensive discovery, granted the defendants' motion to dismiss, because the plaintiffs had "not submitted evidence sufficient to create a genuine issue of material fact as to whether they face a 'certainly impending' risk of identity theft."[140]

In addressing the standing issue, the Fourth Circuit struggled with the issue of actual versus speculative harm, and was swayed by the "attenuated chain of possibilities" rejected in *Clapper*.[141]

> [W]e must assume that the thief targeted the stolen items for the personal information they contained. And in both cases, the thieves must then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to

---

[133] Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017), *cert. denied sub nom*. Beck v. Shulkin, 137 S.Ct. 2307 (2017).
[134] *Id.* at 266.
[135] *Id.*
[136] *Id.* at 267.
[137] *Id.*
[138] Amended Complaint, Beck v. Shinseki, et al., No. 3:13-CV-999-TLW (D.S.C. July 1, 2013).
[139] *Beck*, 848 F.3d at 267.
[140] *Id.* at 267–68 (citing *Clapper*, 568 U.S. at 422.).
[141] 568 U.S. at 410.

> use that information to steal their identities. This 'attenuated chain' cannot confer standing.[142]

The court put a heavy burden on plaintiffs. Recognizing that the breaches occurred years before, the court noted the "plaintiffs have uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information"[143] and "'as the breaches fade further into the past,' the Plaintiffs' threatened injuries become more and more speculative."[144] Telling is the fact that the court included this quote from the district court in the *Zappos* breach. "[T]he passage of time without a single report from Plaintiffs that they in fact suffered the harm they fear must mean something."[145]

The plaintiffs did manage to argue that there is "no need to speculate"[146] because they alleged that their personal information had been stolen. The court explicitly accepted that to be true, but held "the mere theft of [the laptop and personal information], without more, cannot confer Article III standing."[147] The court cited *Randolph v. ING Life Ins. & Annuity Co.*,[148] persuaded by the argument in that case that "although plaintiffs clearly alleged their information was stolen by a burglar, they did 'not allege that the burglar who stole the laptop did so in order to access their [i]nformation, or that their [i]nformation ha[d] actually been accessed since the laptop was stolen.'"[149]

d. Eighth Circuit

In June and July of 2014, the network that processes credit card transactions for 1,045 grocery stores was hacked, and names, account numbers, expiration dates, card verification value (CVV) codes, and personal identification numbers were exfiltrated.[150] Interestingly, the court stated: "[b]y harvesting the data on the network, the hackers stole customers' Card Information."[151]

In September of the same year, defendants announced a second data breach had occurred, with different malicious software onto the

---

[142] *Beck*, 848 F.3d at 275.
[143] *Id.* at 274–75.
[144] *Id.* at 275.
[145] In re Zappos.com, 108 F. Supp. 3d 949, 958 (D. Nev. 2015).
[146] *Beck*, 848 F.3d at 275.
[147] *Id.* at 274–75.
[148] *Id.* (citing Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 7–8 (D.D.C. 2007).).
[149] *Id.*
[150] In re SuperValu, Inc., 870 F.3d 763, 766 (8th Cir. 2017).
[151] *Id.*

same network.[152] Sixteen plaintiffs sued, and the district court dismissed the complaint without prejudice, finding that "none of the plaintiffs had alleged an injury-in-fact and thus they did not have standing."[153]

The court considered the injury-in-fact and traceability issues. However, the court was troubled by the eventual *use* of the stolen information, rather than the fact that the information was stolen in the first place. "Drawing all inferences in the plaintiffs' favor, we are satisfied that the complaint sufficiently alleges that the hackers stole plaintiffs' Card Information. Plaintiffs, however, ask us to go further and conclude that the complaint has adequately alleged that their Card Information has been misused."[154]

Great weight was placed upon the risk of identity theft and credit card fraud, and whether it had occurred or would likely occur in the future. All parties agreed that identity theft would constitute an injury-in-fact. What they seemed to miss is that there are other injuries involving data theft (e.g. extortion, loss of privacy), besides the fact that data theft is theft, too. Note this comment from the court, which seems to miss the mark: "[o]ur task is to determine whether plaintiffs' allegations plausibly demonstrate that the risk that plaintiffs will suffer future identity theft is substantial."[155]

In trying to pigeonhole a data breach into an identity theft claim, all parties and the courts miss the fact that data has been misappropriated, and that misappropriation is a current injury.

VI. AN INCORRECT UNDERSTANDING OF THE NATURE OF CYBERDAMAGES?

We began by discussing the theft of a bicycle, the theft of a flash drive, and the theft of the information contained on the flash drive. The first two cases are relatively easy; the third causes us some pause. When information is wrongfully accessed, is there injury?

That the plaintiffs have suffered a harm in most data breach cases is not in question. If these cases involved only the hacker and the plaintiff, and the hacker lifted the information directly from the plaintiff, we would see very clearly any number of theories for liability,

---

[152] *Id.*

[153] *Id.* at 767.

[154] *Id.* at 769.

[155] *Id.* at 770.

including intrusion upon seclusion,[156] appropriation of another's identity or likeness,[157] and, in some cases, theft.[158]

When the plaintiff's information is taken from a trusted third party, courts have struggled to 1) find the injury, especially absent actual identity theft, although this trend is changing as we become more familiar with data breaches, and 2) to assign blame for the injury upon the third party. We see several reasons why.

First, injuries in the data breach cases sometimes involve actual monetary damage, but many times do not (or the monetary damage is too attenuated from the breach to be able to meet the causation requirement). Sometimes the harm of identity theft is mitigated by the victim or a third party, and the public (and the courts?) think, "Whew!"

We shouldn't find a lot of solace in this. Legislatures the world over have looked at these breaches and listened to their constituents. Business leaders lose sleep over the thought that, in the current political climate, customers are demanding security and privacy, and when a breach occurs, they expect compensation, sometimes despite the best efforts of the business to keep their data safe.[159]

Second, courts and law makers are trying to understand the nature of the harm. Is it trespass? Invasion of privacy? Breach of trust? Conversion? Which legal theory is the correct one, and how does that help us understand when an injury is redressable, and when it's not?

Property (if data is property?)[160] is copiable, so what is the harm in another copy? Just change your password! But this does not agree with our legal history of theft or tort. It doesn't agree with the public's notion of privacy (even when that privacy is crowd-shared and tweeted for all to see).

Third, courts and companies are struggling with the concept of damage. If there is an injury, how much is it worth? We've rushed headlong into a digital society, with all its apps and connectivity, but the law is still trying to decide what the ground rules are. Are we open with no secrets, or are there still some things that are not for public viewing? If so, how much are those things worth?

---

[156] *See* RESTATEMENT (SECOND) OF TORTS §652B (1977); Plaxico v. Michael, 735 So. 2d 1036 (Miss. 1999).

[157] Joe Dickerson & Associates, LLC v. Dittmar, 34 P.2d 995 (Colo. 2001).

[158] *See, e.g.*, Univ. Sports Publ'n Co. v. Playmakers Media Co., 725 F. Supp. 2d 378 (S.D.N.Y. 2010).

[159] *See, e.g.*, Gabriel Torok, *Data Breaches in 2019: Why the Hackers are Winning (and What You Can Do About It)*, PREEMPTIVE (Jan. 9, 2019), https://www.preemptive.com/blog/article/1089-data-breaches-in-2019-why-the-hackers-are-winning-and-what-you-can-do-about-it/106-risk-management.

[160] Jeffrey Ritter and Anna Mayer, *Regulating Data As Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220 (2017).

Finally, are we looking at damages from the wrong point of view? A hacker may steal information for a number of reasons, including 1) to sell the information, 2) to shut down a computer or network, 3) to extort the owner of the information, or 4) to use the information herself. In each case, we see the hacker receiving enrichment wrongfully, while at the same time we may look at the individual and (legally) see no injury.

CONCLUSION

"[T]he average lawyer is not merely ignorant of science, he or she has an affirmative aversion to it."[161]

"As a general matter, lawyers and science don't mix."[162]

We start with these two statements for both entertainment value and as a cautionary tale. On the one hand, it's amusing to think that the law (and lawyers and courts) has an aversion to technology and science when we rush into the breach whenever technology doesn't work. The speed with which putative class actions are formed seems to prove that no such enmity exists.

On the other hand, the law (and lawyers and the courts) are creatures of habit and precedent. We love tying technology, science, the internet, and anything intangible to theories that we have grown to love and adore for centuries. When we do so, sometimes we find that the fit is more "round peg in a square hole" than "hand in glove."

There are a lot of square holes in breach litigation. Statutes can be vague or use language that no longer applies. Common law actions such as bailment or trespass don't quite fit when there is no land, chattel, or maybe even property to speak of.

As we face more data breaches each year, courts and legislatures will have to confront the tough issues of damage and liability, standing and causation, and injury in a data driven world.

> Digital freedom stops where that of users begins... Nowadays, digital evolution must no longer be a customer trade-off between privacy and security. Privacy is not to sell, it's a valuable asset to protect.[163]

As they confront those issues, courts and legislatures will have to reconcile our changing notions of what constitutes harm from cyber theft. Because much of the litigation is one victim suing another, the

---

[161] DAVID L. FAIGMAN, LEGAL ALCHEMY: THE USE AND MISUSE OF SCIENCE IN LAW XI (1999).

[162] Peter Lee, *Patent Law and the Two Cultures*, 120 YALE L.J. 2, 4 (2010).

[163] Nataly Yosef, *Privacy Concerns Featuring: The Battle Over BIPA Claims*, U. OF ILL. J. MARSHALL L. REV. (2018), https://lawreview.jmls.edu/privacy-concerns-featuring-the-battle-over-bipa-claims/ (quoting Stephane Nappo).

real harm tends to be obscured. Instead we ask whether one of the victims was negligent in protecting the data, and whether the other victim really had anything stolen. Since the thief is long gone, we tend to look for justice from the only people who are left.