# LAW FIRM CYBERSECURITY: THE STATE OF PREVENTATIVE AND REMEDIAL REGULATION GOVERNING DATA BREACHES IN THE LEGAL PROFESSION

MADELYN TARR[†]

ABSTRACT

*With the looming threat of the next hacking scandal, data protection efforts in law firms are becoming increasingly crucial in maintaining client confidentiality. This paper addresses ethical and legal issues arising with data storage and privacy in law firms. The American Bar Association's Model Rules present an ethical standard for cybersecurity measures, which many states have adopted and interpreted. Other than state legislation mandating timely disclosure after a data breach, few legal standards govern law firm data breaches. As technology advances rapidly, the law must address preventative and remedial measures more effectively to protect clients from data breaches caused by outdated or ineffective cybersecurity procedures in law firms. These measures should include setting a minimum standard of care for data security protection and creating a private cause of action for individuals whose personal information has been improperly accessed because of a failure to comply with those standards.*

## INTRODUCTION

At the intersection of exponentially growing technology and online data storage, hacking efforts have increasingly targeted personal information stored by large companies stuck in the past. Recently, a growing number of companies' outdated security systems have been hacked. Hackers are selling customers' personal information in mass quantities. Law firms have been targeted because their storage of confidential information has created an attractive temptation for hackers.[1] There is no set of uniform legal standards for remedying the harms caused

[†] Duke University School of Law, J.D./LLM in Law and Entrepreneurship expected May 2018; B.A. in International Studies and Spanish, University of Miami, 2014.

[1] Karen Painter Randall & Steven A. Kroll, *Getting Serious About Law Firm Cybersecurity*, N. J. LAW. THE MAG., June 2016, at 54–55; *see also* DREW SIMSHAW & STEPHEN S. WU, AMERICAN BAR ASSOC. SECTION OF LABOR AND EMP'T LAW, ETHICS AND CYBERSECURITY: OBLIGATIONS TO PROTECT CLIENT DATA 2–4 (2015).

by security breaches,[2] as legislation has not caught up with technological developments and large corporations typically settle cases before trial, hindering the development of legal precedent. Nonetheless, some existing client confidentiality and professional ethical standards govern the legal profession's interactions with clients.

This brief will address the current cybersecurity regulations, and lack thereof, on attorneys' conduct. Traditional lawsuits prompted by data breaches have mostly appeared against large corporations like Target or Sony.[3] Although law firms are hacked as frequently,[4] they are not being sued, and the details of any consequential data breaches remain hidden from the public eye. There is little state-level regulation of data security, and federal regulation of data security is nonexistent.[5] Massachusetts is known for setting a benchmark in data security regulation, but the Office of the Massachusetts Attorney General opposed Congress's attempt at enacting The Data Security and Breach Notification Act of 2015 which would have created nationwide data breach notification standards.[6] The Attorney General of Massachusetts, Maura Healey, stated that the reason for opposition was that a lax national standard, as the law proposed, would

---

[2] Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 406 (2016).

[3] *See* Ahiza Garcia, *Target Settles for $39 Million over Data Breach*, CNN MONEY (Dec. 2, 2015, 5:48 PM), http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/; Edvard Pettersson, *Sony to Pay as Much as $8 Million to Settle Data-Breach Case*, BLOOMBERG (Oct. 20, 2015), https://www.bloomberg.com/news/articles/2015-10-20/sony-to-pay-as-much-as-8-million-to-settle-data-breach-claims.

[4] Melissa Meleske, *1 in 4 Law Firms Are Victims of a Data Breach*, LAW360 (Sept. 22, 2015, 7:16 PM), http://www.law360.com/articles/705657/1-in-4-law-firms-are-victims-of-a-data-breach (stating that about 150 hacking incidents involving law firms occurred between May 2014 and May 2015).

[5] Another way that law firm data protection is regulated is through their clients' data privacy obligation. When firms represent clients whose data storage is subject to privacy regulation, such as compliance with the Health Insurance Portability and Accountability Act (HIPAA), if the firms gain access to that data and store it, the clients' privacy responsibilities pass through to their attorneys. The right of action is public with only civil and criminal penalties so clients are not able to sue law firms for damages caused by noncompliance. Eric A. Hawley, *Cyber Security and Disaster Recovery Issues for Law Firms*, HOUSTON LAW., Jan/Feb. 2016, at 18, 19; *see also* Peter J. Arant, *Understanding Data Breach Liability: The Basics Every Attorney Should Know*, 40 MONT. LAW., Feb. 2015, at 8; Health Insurance Portability and Accountability Act of 1996 (HIPAA) P.L. No. 104-191, 110 Stat. 1938.

[6] Divonne Smoyer & Kimberly Chow, *Q&A with Massachusetts AG Maura Healey*, INT'L ASSOC. OF PRIVACY PROF'LS (Aug. 23, 2016), https://iapp.org/news/a/qa-with-massachusetts-ag-maura-healy/.

undercut the progress that Massachusetts and other states have made because the law would preempt state laws with a vague national law that leaves consumers unprotected.[7]

This new area of law is constantly evolving and legislation will have to catch up to technology to provide proper remedies for victims of data breaches caused by lax cybersecurity policies. Recently filed lawsuits have begun to creatively address these gaps, but there needs to be a legal standard of responsibility that allows claims relating to both preventative measures and post-breach accountability to succeed more frequently in court. State legislatures should require companies to comply with a minimum standard of care and create a private cause of action for individuals whose personal information has been compromised as a result of noncompliance with that standard. Courts should move toward an interpretation of harm caused by data breach as sufficiently imminent to pass beyond the threshold of purely speculative harm and confer Article III standing. This would provide adequate common law remedies to individuals under theories of negligence.

## I. ETHICAL STANDARDS

The American Bar Association ("ABA") has made an effort to incorporate cybersecurity into their Model Rules of Professional Conduct. In 2012, the ABA amended Rule 1.6(c) to state that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[8] Comment 18 of 1.6 enumerates factors to consider in determining whether an attorney has made reasonable efforts, but the list is not exhaustive.[9] The Comment to Rule 1.1 titled "Competence" states that "a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."[10] The ABA was purposeful in its choice of language to allow the rule to evolve, understanding that any specific reference to technology might quickly become outdated.[11] Many state bar associations have adopted these

---

[7] *Id.*

[8] MODEL RULES OF PROF'L CONDUCT r. 1.6 (AM. BAR ASS'N, 2012).

[9] *Id.* ("Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients").

[10] *Id.*

[11] Myles G. Taylor, *Seeing Clearly? Interpreting Model Rule 1.6(c) for Attorney Use of Cloud Computing Technology*, 45 MCGEORGE L. REV. 835, 848–49 (2014).

changes into their respective ethical rules.[12] The imprecision of the "reasonable efforts" language, however, has led to differing interpretations.

Some of the states that have adopted the 2012 changes or a similar variation have issued Ethics Opinions as a guide to interpreting 1.6(c). Massachusetts, for example, interpreted the rule in the context of using Google Docs for a data storage solution.[13] The Committee on Professional Ethics determined that Google Docs would be an appropriate storage solution if the attorney "undertakes reasonable efforts to ensure that the provider's data privacy policies, practices and procedures are compatible with Lawyer's professional obligations."[14] "Reasonable efforts" include examining the provider's policies and procedures, making sure the terms of use prohibit unauthorized access, ensuring that the lawyer has access to the data past termination of the use of service, examining the provider's own cybersecurity efforts, and staying up to date with all of the above.[15] Nevertheless, the Committee's conclusion is unclear. Ultimately, the lawyer must use his sound professional judgment to determine whether the service is compatible with his ethical obligations.

While New York has not adopted the amendments, their Ethics Opinion 1019 interprets Comment 17 to Rule 1.6[16] which states that in sending confidential information, "the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."[17] New York listed four steps to consider in determining reasonable care: (1) "[e]nsuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security", (2) investigating the provider's own security measures, (3) using available technology to prevent foreseeable infiltration attempts, and (4) looking into the provider's ability to erase data after the business relationship is terminated.[18]

---

[12] *See generally* CPR POLICY IMPLEMENTATION COMM., AM. BAR ASS'N VARIATIONS OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT: RULE 1.6: CONFIDENTIALITY OF INFORMATION (2016).

[13] Mass. Bar Ass'n Comm. on Prof'l Ethics, Op. 12-03 (2012).

[14] *Id.*

[15] *Id.*

[16] Rule 1.6(c) states that " [a] lawyer shall exercise reasonable care to prevent the lawyer's employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidential information of a client." MODEL RULES OF PROF'L CONDUCT r. 1.6 (AM. BAR ASS'N, 2012).

[17] N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 1019 (2014).

[18] *Id.*

Florida's ethics opinion on the rule turns to other states' interpretations in addressing cloud computing.[19] In particular, Florida adopts New York's list of steps to determine reasonable care.[20] It emphasizes the practicality of Iowa's Ethics Opinion 11-01.[21] The Iowa opinion sets forth questions that lawyers should ask when considering using information technology services, including accessibility inquiries on access, legal issues, financial obligations, and termination of services, and data protection inquiries on password protection, public access, and data encryption.[22] The Florida opinion adds that the lawyer should consider whether additional security measures are necessary in cases of particularly sensitive information.[23]

This sampling of interpretations shows the variation among what constitutes "reasonable efforts" in each state. There is no consistent standard, or even a definitive line to judge attorneys' behavior with respect to data security and confidentiality. Even though ethical rules by nature consist of flexible standards, the risk to client confidentiality, a pillar of legal ethics, should warrant more predictable standards. It remains to be seen how helpful the current standards will be as law firms face a growing threat of hacking.

## II. DATA BREACH NOTIFICATION LAWS

Forty-seven states have enacted data breach notification statutes.[24] These statutes require governmental, educational and private entities to notify affected individuals of data breaches compromising personally identifiable information. The statutes vary on which entities must comply, the definition of personal information, the definition of a breach, notification requirements, and exemptions.[25] Despite the inconsistencies, these statutes are the closest thing to a universal cybersecurity regulation protecting consumers. However, the laws do not mandate preventative measures. They mandate notification of data breaches to consumers,

---

[19] *See* Fla. Bar Ass'n Prof'l Ethics Comm., Op. 12-3 (2013).
[20] *See id.*
[21] *See id.*
[22] *See* Iowa State Bar Ass'n Comm. on Ethics and Practice Guidelines, Op. 11-01 (2011).
[23] Fla. Bar Ass'n Prof'l Ethics Comm., Op. 12-3 (2013).
[24] *See Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGS., (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[25] *Id.*

which only becomes relevant after a security breach has already occurred.[26] Only some states grant a private cause of action.[27]

In terms of notification timing, the statutes range in language from "most expedient time possible without unreasonable delay," to "immediately," to "as soon as reasonably practical," and to combinations of the three phrases. Ohio and Wisconsin give a set limit of 45 days to notify consumers of a breach of personal information.[28] The statutes of California, New York and Texas offer a representative spectrum of data breach notification statutes. All three cover unauthorized access to personally identifying information, but Texas and California include medical data in the definition of personal information.[29] Neither New York nor Texas offer a private cause of action, but while Texas only allows their Attorney General to enforce compliance, New York allows their Attorney General to bring an action on behalf of the victims.[30] The only penalties available in Texas are civil fines and injunctive or equitable relief. New York allows both of those along with recovery of consequential financial losses to the victim.[31] California allows civil remedies, through a private cause of action, to customers who were injured by a statutory violation.[32]

Through the enforcement inconsistencies and the fact that the statutes only cover consequences from delay of notification—not from the actual breach itself—these statutes fail to adequately incentivize entities to increase preventative data security measures.

Most of the statutes prescribe civil or criminal penalties for failure to promptly notify customers. Only 10 states, however, give a private cause of action to consumers harmed by the failure to comply with

---

[26] CAL. CIV. CODE § 1798.82 (West 2016); TEX. BUS. & COM. CODE ANN. § 521.002 (West 2009); N.Y. GEN. BUS. LAW § 899-aa (McKinney 2013); *see generally State Data Security Breach Notification Laws*, MINTZ LEVIN (2016), https://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf.

[27] *Id.*

[28] OHIO REV. CODE ANN. § 1349.19 (West 2007); WIS. STAT. ANN. § 134.98 (West 2008); *see generally State Data Security Breach Notification Laws*, *supra* note 26.

[29] CAL. CIV. CODE § 1798.82; TEX. BUS. & COM. CODE ANN. § 521.002; N.Y. GEN. BUS. LAW § 899-aa; *see generally State Data Security Breach Notification Laws*, *supra* note 26.

[30] TEX. BUS. & COM. CODE ANN. § 521.151; N.Y. GEN. BUS. LAW § 899-aa; *see generally State Data Security Breach Notification Laws*, *supra* note 26.

[31] TEX. BUS. & COM. CODE ANN. § 521.151; N.Y. GEN. BUS. LAW § 899-aa; *see generally State Data Security Breach Notification Laws*, *supra* note 26.

[32] CAL. CIV. CODE § 1798.82; *see generally State Data Security Breach Notification Laws*, *supra* note 26.

notification requirements after an unauthorized data access.[33] Moreover, courts have been reluctant to find injury caused by late notification in violation of the statutes.[34] While the threat of a penalty might encourage companies to adopt stricter cybersecurity measures, most of the statutes do little to address the damage caused to consumers.[35]

## III. STATE STANDARD OF CARE STATUTES

### *A. Overview*

California is one of the minority of states with standard of care laws for businesses maintaining personal information on state residents. California Civil Code 1798.81.5(b) states that "[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."[36] This statute also includes a cause of action for private citizens who have suffered harm from a violation.[37]

Other states have enacted standard of care statutes, but most are enforced through penalties for noncompliance and do not give a private cause of action to individuals. For example, in 2015, Rhode Island enacted the Identity Theft Protection Act, which requires businesses to implement a risk-based information security program that contains reasonable procedures and practices.[38] Only the Attorney General of Rhode Island, however, can bring an action against violating companies if it is in the public interest.[39] Similarly, in 2010, Massachusetts enacted a statute with the purpose of protecting personal information by mandating the adoption of a comprehensive information security program by any person who owns or licenses personal information about a Massachusetts resident.[40] Once again, only the Attorney General of Massachusetts may bring an enforcement action against a noncomplying person.[41] Massachusetts has

---

[33] S*ee generally State Data Security Breach Notification Laws*, *supra* note 26.
[34] *See, e.g.*, Corona v. Sony Pictures Ent't, Inc., No. 14-CV-09600 RGK, 2015 WL 3916744 (C.D. Cal. June 15, 2015); Dugas v. Starwood Hotels & Resorts Worldwide, Inc., No. 3:16-cv-00014-GPC-BLM slip op. (S.D. Cal. Nov. 3, 2016); *In re* Sony Gaming Networks and Customer Data Sec., 996 F.Supp.2d 942, 965 (S.D. Cal 2014).
[35] *In re* Sony Gaming Networks and Customer Data Sec., 996 F.Supp.2d at 965.
[36] CAL. CIV. CODE § 1798.81.5(b).
[37] *Id.*
[38] 11 R.I. GEN. LAWS. ANN. § 11-49.3-2 (West 2015).
[39] *Id.* § 11-49.3-5.
[40] 201 MASS. CODE. REGS. 17.01–05.
[41] MASS. GEN. LAWS ANN. ch. 93H § 6 (West 2007).

some of the most stringent data breach regulations,[42] but even so, public enforcement only results in injunctive relief or civil penalties, with no relief to the victims of the data breach.[43]

### *B. Article III Standing*

The first step in obtaining a remedy for a breach of a state standard of care statute is to prove standing under Article III of the U.S. Constitution, which requires injury-in-fact.[44] Under Article III, "a plaintiff must show (1) it has suffered an "injury in fact" that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision."[45] Under the Supreme Court's standard in *Clapper v. Amnesty International USA*, a threatened injury must be "certainly impending" to constitute imminence in injury-in-fact.[46] The imminence requirement ensures that the alleged injury is not speculative or just a claim of possible future injury.[47] It is important to note that the court's Article III standing analysis is only a preliminary review of the merits of the case; the parties must subsequently litigate the substantive issues before any damages can be awarded.

An influential decision from the Northern District of California abandoned previous courts' tendency to recognize consumer claims of compromised but not misused personal information.[48] This case, *In re Adobe Systems, Inc. Privacy Litigation*, determined that plaintiffs had standing to bring a class action suit against a corporation for failure to maintain reasonable data security under § 1798.81.5(b).[49] Threatened harm was enough of a defined threat to be considered imminent and requiring plaintiffs to wait for hackers to misuse the accessed information

---

[42] Smoyer & Chow, *supra* note 6.

[43] Lisa M. Ropple, et. al., *Massachusetts Adopts Strict Security Regulations Governing Personal Information*, 2009 PRIVACY & DATA SECURITY L.J., 318, 324.

[44] U.S. CONST. art. 3, § 2, cl. 1; Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000). For further discussion on injury-in-fact, see *infra* Part IV.A.

[45] *Friends of the Earth*, 528 U.S. at 180–81.

[46] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013).

[47] *Id*.

[48] *Class Actions and Other Security Breach Litigation*, 3 E-COMMERCE AND INTERNET LAW § 27.07 (2015).

[49] *In re* Adobe Sys., Inc. Privacy Litig., 66 F.Supp.3d 1197, 1220 (N.D. Cal. 2014).

weakens evidence of connection between the misused data and the defendant.[50]

*Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, after similarly granting standing to the plaintiffs, considered the claim that the defendant violated their legal duty under § 1798.81.5(b) by failing to implement proper security protocols.[51] The court found that because the plaintiffs had sufficiently alleged that Starwood failed to encrypt customer data in accordance with reasonable industry standards, they had plausibly alleged a cause of action to survive defendants' motion to dismiss.[52]

Overall, though California establishes a standard of care that companies must comply with, it is difficult to establish adequate injury-in-fact for standing, and even more difficult to properly allege a cause of action under the statute. It remains to be seen how courts will construe claims of injuries caused by violations of the statute and until then, companies (law firms included) will have little incentive to increase their data security measures.

## IV. COMMON LAW REMEDIES

Customers affected by hacks of large corporations have prevailed in claims based on a theory of negligence, which involves duty, breach of duty, cause, and evidence of injury. While these cases are often highly publicized, most companies reach a settlement agreement before the case arrives in court. Claims against law firms, on the other hand, can be sealed to prevent exposure of confidential client information.[53] Combined with the novelty of data breach issues, these circumstances contribute to a sparse record of judicial opinions with which to advance the field.

### *A. Article III Standing*

Negligence and breach of implied contract are the most frequently used common law claims for affected individuals to recover damages after a data security breach. Prior to evaluating the merits of these claims, courts must consider the question of standing under Article III, which requires injury-in-fact, causation, and redressability, as described above.[54] There must have been an invasion of a legally protected interest which is

---

[50] *Class Actions and Other Security Breach Litigation*, *supra* note 48, § 27.07.
[51] Dugas v. Starwood Hotels & Resorts Worldwide, Inc., No. 3:16-cv-00014-GPC-BLM slip op. at 10 (S.D. Cal. Nov. 3, 2016).
[52] *Id.* at 10–11.
[53] Allison Grande, *Edelson Targets Chicago Law Firm over Lax Data Security*, LAW360, (May 5, 2016), http://www.law360.com/articles/793028/edelson-targets-chicago-law-firm-over-lax-data-security.
[54] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992).

particularized and concrete, as well as actual and imminent.[55] There must be a causal connection between the injury and the claimed wrongdoing.[56] And the injury must be likely to be redressed by a verdict in the plaintiff's favor.[57]

The injury-in-fact requirement has become the main obstacle in litigating data breach cases. Multiple courts have dismissed claims for lack of standing because the potential risk of identity theft through unauthorized access of personal information is not considered an injury-in-fact.[58] As mentioned above, a threatened injury must be "certainly impending" to constitute imminence in injury-in-fact.[59] In *Reilly v. Ceridan Corp.*, the Third Circuit dismissed a claim for damages caused by a security breach for lack of Article III standing.[60] The court concluded that "allegations of hypothetical, future injury are insufficient to establish standing" and until the alleged injury actually occurs, the information has not been misused and no injury has occurred.[61]

The Ninth Circuit has allowed data breach claims, given that the plaintiff faces a credible threat of harm that is real and immediate.[62] In *Krottner v. Starbucks Corp.*, the Ninth Circuit held that the plaintiffs had "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data" and granted Article III standing.[63]

However, the *Krottner* decision is limited in application. For instance, in *Antman v. Uber Technologies, Inc.*, the District Court for the Northern District of California held that the plaintiff's allegations of injury were insufficient because only names and driver's license numbers were stolen in Uber's data breach.[64] Even though the court acknowledges that

---

[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] Arant, *supra* note 5, at 10; Stephen J. Rancourt, *Hacking, Theft, and Corporate Negligence: Making the Case for Mandatory Encryption of Personal Information*, 18 TEX. WESLEYAN L. REV. 183, 188–194 (2011).
[59] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013).
[60] Reilly v. Ceridan Corp., 664 F.3d 38 (3rd Cir. 2011).
[61] *Id.* at 42.
[62] *Id.*
[63] Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010). Even though the Ninth Circuit granted standing, the court denied that danger of future harm without present injury, under Washington law (which does not have a standard of care statute with a corresponding private right of action), would support a negligence claim.
[64] Antman v. Uber Techs., Inc., No. 3:15-cv-01175-LB, 2015 WL 6123054, at *11 (N.D. Cal 2015).

*Krottner* was the relevant precedent for injury-in-fact Article III standing, the court stated that "[w]ithout a hack of information such as social security numbers, account numbers, or credit card numbers, there is no obvious, credible risk of identity theft that risks real, immediate injury."[65]

*Dugas v. Starwood Hotel & Resorts Worldwide, Inc.* took an even more limited view of *Krottner*. Because the plaintiff only alleged the theft of names, addresses, billing information, and credit card numbers, the District Court for the Southern District of California concluded that the information stolen was insufficient for a third-party to open up or access any personal accounts.[66] Therefore, the personal information stolen was not in itself sufficient to allege future harm and establish injury-in-fact.[67] Theoretically the affected consumers were safe from unauthorized access to their personal accounts. But in reality, stolen information that consumers trusted companies to keep private could be used for nefarious purposes beyond identity theft through access to personal accounts.[68]

The Fourth Circuit, in *Beck v. McDonald*, reasoned that mere theft is insufficient to confer standing: for the plaintiffs to suffer the potential harm claimed, the court must assume that the thief targeted the data for the personal information it contained, selected the plaintiff's specific personal information, and successfully used it for identity theft.[69] This "attenuated chain of possibilities" was too far removed to be certainly impending.[70] The second part of the court's analysis considered that standing may be found when there is a substantial risk of future harm.[71] Yet even so, the allegation that 33% of health-related data breaches resulted in identity theft, assumed to be true, was not enough of a substantial risk to confer standing because 66% of those affected would suffer no harm.[72]

Conversely, the Seventh Circuit has recognized a threat of future harm or a risk of future harm caused by the defendant's actions as sufficient to support standing.[73] Following the Seventh Circuit's

---

[65] *Id.* at *10–11.
[66] Dugas v. Starwood Hotels & Resorts Worldwide, Inc., No. 3:16-cv-00014-GPC-BLM slip op. at 5 (S.D. Cal. Nov. 3, 2016).
[67] *Id.*
[68] Natasha Bertrand, *Here's What Hackers Do with Your Data*, BUS. INSIDER (Oct. 14, 2014), http://www.businessinsider.com/hackers-are-selling-your-data-in-highly-sophisticated-black-markets-2014-10.
[69] Beck v. McDonald, No. 15-1395, No. 15-1715, 2017 WL 477781, at *8 (4th Cir. Feb. 6, 2017).
[70] *Id.*
[71] *Id.* at *9.
[72] *Id.*
[73] Karen A. Popp & Edward R. McNicholas, *Standing to Assert Privacy and Data Security Harms, in* 12 BUSINESS AND COMMERCIAL LITIGATION IN FEDERAL

reasoning, the Southern District of California in *Dugas* recognized, despite their limited view of future harm, that another injury that has been considered injury-in-fact was "lost time and expenses associated with 'mitigat[ing] the actual . . . consequences of the data theft.'"[74] Based on the Seventh Circuit decision that loss of time by a plaintiff for having to mitigate misuse of credit card information constituted injury-in-fact[75], the court concluded that the plaintiff had Article III standing.[76]

Similarly, the Sixth Circuit in *Galaria v. Nationwide Mutual Insurance Company* stated that "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints."[77] Recognizing that it is unreasonable to require plaintiffs to wait for actual misuse of their information, the court found that mitigation costs constituted actual injury.[78] While remedies under these theories would be limited, legitimizing mitigation damages would move precedent toward recognizing data breaches as causing imminent and quantifiable damage to consumers and holding organizations accountable for lax security policies.

A recent case, *Khan v. Children's National Health System*, elaborated on a proper allegation of injury-in-fact: the plaintiff must "put forth facts that provide either (1) actual examples of the use of the fruits of the data breach for identity theft, even if involving other victims; or (2) a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud."[79] The U.S. District Court for the District of Maryland denied standing to the plaintiff under not only this theory, but also against the argument that the expense of guarding against identity theft was an injury-in-fact. Similarly, the U.S. District Court for the District of Nevada in *In re Zappos.com, Inc.*, held that the purchase of credit monitoring services as a result of breach did not constitute injury-in-fact because "in order for costs incurred in an effort to

---

COURTS § 122:28 (Am. Bar Assoc. Section of Litig. ed., 4th ed. 2016). *See generally* Pisciotta v. Old Nat'l Bancorp., 499 F.3d 629 (7th Cir. 2007).

[74] *Dugas*, slip op. at 6.

[75] The court noted that the Ninth Circuit had yet to address anxiety and lost time to avoid financial loss as constituting injury. *Id.*

[76] *Id.*

[77] Galaria v. Nationwide Mut. Ins. Co., Nos. 15-3386/3387, 2016 WL 4728027, at *3 (6th Cir. Sept. 12, 2016).

[78] *Id.*

[79] Khan v. Children's Nat'l Health Sys., 2016 WL 2946165, at *5 (D. Md. May 18, 2016).

mitigate the risk of future harm to constitute an injury-in-fact, the future harm being mitigated must itself be imminent."[80]

Taking a step back, these cases interpret injury-in-fact for Article III standing, which is only the first obstacle to recovery of damages. They show that many lawsuits concerning data breaches are not granted Article III standing. Even if the courts do grant standing, the parties still have to litigate the substantive issues, and the court has to rule for the victim plaintiffs before any damages are awarded. However, of the cases granted standing, most are not litigated but settled amongst the parties. There may be two reasons for settling: (1) litigation costs are high, and (2) with such little precedent, the risk of an unfavorable decision for victim plaintiffs is too high to forego a definite remedy through settlement. Essentially, the result is a dearth of precedent for data breach case, hindering the natural development of the law that occurs when courts examine new technological issues.

### *B. Common Law Negligence Claims*

Even if a plaintiff survives dismissal for lack of standing, injury-in-fact for Article III standing alone does not establish adequately pled damages for the cause of action.[81] The economic loss doctrine can also bar a common-law negligence claim.[82] This doctrine states that recovery of damages is precluded unless the data breach is accompanied by personal injury or property damage.[83] And without identity theft or other quantifiable harm, courts have not recognized emotional or dignitary harm as a personal injury supporting standing under the negligence claim.[84] There is no remedy for data breach victims suffering unquantifiable harm, despite the tremendous value society presently places on personal information.

In *Dugas*, after establishing adequate injury for standing, the court considered the plaintiff's negligence claim.[85] The court stated that "[i]n the absence of (1) personal injury, (2) physical damage to property, (3) a special relationship existing between the parties, or (4) some other common law exception to the rule, recovery of purely economic loss is foreclosed."[86] Finding no personal or property injury, and no special relationship, the court dismissed the claim.[87] While companies can avoid

---

[80] *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 960–61 (D. Nev. 2015).
[81] *Dugas*, slip op. at 10.
[82] Arant, *supra* note 5, at 11.
[83] *Id.*
[84] Popp & McNicholas, *supra* note 73.
[85] *Dugas*, slip op. at 12.
[86] *Id.*
[87] *Id.*

litigation by compensating victims through settlements, victims have struggled to receive any judicial remedy for their compromised personal information via negligence claims. In these scenarios, victims are compensated, but any precedential value the lawsuit may have had for data breach negligence claims is lost, leaving an underdeveloped body of case law.

In the legal profession, claims for breach of the duty to act as an ordinary, reasonably prudent lawyer can be presented as the tort of malpractice.[88] Malpractice claims require the victim to prove the conduct fell below the required professional standard.[89] These claims, however, usually result in monetary damages, determined by actual injury.[90] Courts likely would not find attorneys liable in unauthorized disclosure cases, mainly because of a lack of evidence of actual harm.[91] Similarly, malpractice damages must be calculated in accordance with other areas of law, which requires near certainty of the amount of damages.[92] These types of cases have done little to influence law firms with respect to their cybersecurity policies.[93]

In states without as broad a range of technology based litigation as California, the results have been even bleaker. In Louisiana, for example, plaintiffs have made claims for negligence, emotional distress, loss and invasion of privacy, identity theft, harassment, nuisance, fear and anxiety.[94] Yet most of these claims are analyzed as negligence claims, requiring plaintiffs to show actual harm.[95] Even in cases where personal information has been compromised, if it has not been used and the plaintiff cannot prove concrete damages, the claims will be dismissed as speculative.[96]

## V. CYBER INSURANCE

Even though the risk of costly data breach has created a growing liability for companies, many courts are holding that commercial general

---

[88] Travis Andrews, *Technology & Legal Ethics: The Need for Uniform Regulation*, 70 CHARLOTTE L. REV. 185, 196 (2016).
[89] *Id.*
[90] *Id.* at 196–97.
[91] *Id.* at 198–99.
[92] *Id.* at 200–201.
[93] *Id.* at 201. For a discussion of a pending malpractice case, see *infra* Part VI.
[94] Michael S. Finkelstein, *Overview of Data Breach Litigation in Louisiana: A Look into Its Uncertain Future*, 63 LA. B.J. 106, 107–08 (2015).
[95] *Id.*
[96] *Id.*

liability ("CGL") insurance policies do not cover cyber-attacks.[97] In *Zurich American Insurance Company v. Sony Corporation of America*, Sony tried to enforce coverage of its commercial general liability insurance policy after hackers breached its data.[98] The Supreme Court of New York in New York County refused to expand coverage of a CGL policy to cyber-attacks.[99] Similarly, attorney professional liability insurance policies could have gaps in coverage related to loss of client data, recovery, business interruption or cyber extortion threats.[100] Nevertheless, while corporate purchase of cyber insurance has increased dramatically in recent years, law firms are slow to follow.[101] Cyber liability insurance is not only helpful in mitigating the impact of data security failure, but it can include pre-breach services, like breach coaches, cyber-readiness analyses, and security awareness programs.[102]

As the number of lawsuits rises and breach mitigation costs, both regulatory and consequential, increase, more firms will likely invest in cyber liability policies. If so, this could lead to firms taking a more active role in updating their security policies, in accordance with the requisite standard of data security outlined by the policy. Noncompliance could potentially lead to litigation if insurance companies fail to cover firms that do not maintain updated security procedures. In *Columbia Casualty Company (CCC) v. Cottage Health System*, CCC refused to indemnify Cottage Health System after a security breach, arguing that its cyber

---

[97] *Cyber-Insurance: Latest Developments*, INT'L LAW OFFICE, (Nov. 10, 2015), http://www.internationallawoffice.com/Newsletters/Insurance/USA/Mendes-Mount-LLP/Cyber-insurance-latest-developments. However, the Fourth Circuit Court of Appeals held in an unpublished opinion that a medical records company's CGL policy covered the company when it improperly allowed plaintiffs' personal information to be displayed publicly. Because the company published private information electronically, the court held that personal and injury advertising coverage provision of the policy covered the incident. Travelers Indem. Co. of Am. v. Portal Healthcare Sols., LLC, 644 Fed. Appx. 245, 247–48 (2016).

[98] Jim Vorhis & Joan Cotkin, *How Courts Have Decided Coverage Issues in Cyber Insurance Cases*, L.A. LAW., Sept. 2015, at 40.

[99] *Id.*; *see also* Recall Total Info. Mgmt. Inc. et al v. Federal Ins. Co., 147 Conn. App. 450, 462–63 (Conn. App. Ct. 2014) (holding that the personal injury provision of CGL insurance requires not just loss of, but publication of personal information).

[100] Jeffery A. Franklin, *Cyber Insurance for Law Firms*, 33 GP SOLO, no. 3, May/June 2016, at 59.

[101] David L. Hudson Jr., *Net Risk: Cyber Liability Insurance is an Increasingly Popular, Almost Necessary Choice for Law Firms*, ABA J. (Apr. 2015), http://www.abajournal.com/magazine/article/cyber_liability_insurance_is_increasingly_popular_almost_necessary_choice/.

[102] *Id.*

insurance policy covering Cottage Health System required the company to adhere to basic security practices, which they failed to do.[103] These types of preventative security measures, although motivated by the desire to pass liability on to insurance companies, can help to reduce the amount and magnitude of future breaches.

Unfortunately, recent court interpretations of cyber insurance coverage have narrowly construed the scope of the policies. In one of the first cyber insurance coverage rulings, the U.S. District Court for the District of Utah held that a cyber liability policy covering losses caused by an "errors and omissions wrongful act" does not cover non-negligent acts.[104] The court's narrow view that only allegations on a theory of negligence are within the scope of the policy contrasts with many prior interpretations of CGL coverage.[105] Courts have held that CGL insurance typically affords coverage for non-negligence claims, based on the theory that error or omission incorporates more than negligent conduct.[106]

*P.F. Chang's China Bistro, Inc. v. Federal Insurance Company* further showed the holes that cyber insurance policies can have built into them.[107] Here, the U.S. District Court for the District of Arizona held that P.F. Chang's cyber insurance policy's Privacy Injury provision required that the compromised information be owned by the claimant.[108] P.F. Chang's was assessed over $1.9 million in fees from their credit card services intermediary as a result of a data breach.[109] But because the intermediary did not own the personal information—P.F. Chang's did—the insurance policy did not cover P.F. Chang's claim for reimbursement of the intermediary's assessments.[110] The court also found that other claims, which would have been covered, fell under the policy's contractual liability exclusion, which lacked customary carve-outs.[111]

These two cases show a very narrow interpretation of the cyber insurance coverage provisions, compared to cases construing CGL

---

[103] Complaint, Columbia Cas. Co. v. Cottage Health Sys., No. CV 15–03432 DDP (AGRx), 2015 WL 4497730 (C.D. Cal. July 17, 2015).
[104] Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc., 156 F.Supp.3d 1330, 1334–35 (2016).
[105] Roberta D. Anderson, *Five Takeaways from the First Cyber Insurance Case*, LAW360 (May 18, 2015, 10:22 AM), https://www.law360.com/articles/656256/5-takeaways-from-the-first-cyberinsurance-case.
[106] *Id.*
[107] P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM slip op. (Dist. Ariz. May 31, 2016).
[108] *Id.* at *5–7.
[109] *Id.* at *2.
[110] *Id.* at *5–7.
[111] *Id.* at *7–8.

policies, and highlight two problems. First, cyber insurance policyholders must anticipate potential holes in in their policies because a lack of industry standard has led to custom carve-outs and unexpected exclusions to coverage. Second, without much history of court guidance in interpretation, policyholders may be unsure of the scope of their coverage and may find out too late, and after much litigation, that a data breach is not covered by their policy.

## VI. THE LEGAL FUTURE OF PREVENTATIVE AND REMEDIAL MEASURES AMIDST A GROWING THREAT OF DATA BREACH

Overall, a significant regulatory gap exists in the area of law firm data storage protection. With statutory and common law remedies rarely recovering damages for victims of cybersecurity breaches, litigation strategies have had to get more creative. In a current case, *Shore v. Johnson and Bell*, a recently unsealed complaint[112] revealed claims against a law firm for breach of contract, malpractice, unjust enrichment and breach of fiduciary duty for not adequately protecting client data from exposure.[113] The complaint seeks injunctive relief and damages through a theory that clients have been overpaying for legal services which should have included data protection.[114] The firm representing the plaintiff appears to be seeking improvement in law firm data security efforts and hopefully will pursue litigation over settlement. Through their novel theory that clients have been overpaying for legal services, monetary damages may be more easily quantifiable and as a result, the court may be more receptive to recognizing actual injury.

In New York, a couple is suing their attorney for using an AOL account and failing to use protective measures, leading to malware infecting her computer.[115] The clients, engaging in a real estate purchase, were contacted by cybercriminals pretending to be the property seller's attorney and asked to make a deposit of $1.9 million on the property.[116]

---

[112] The complaint was originally temporarily sealed because it "reveal[ed], in explicit detail, where and how [Defendant] had left its clients' confidential information unsecured and unprotected." On December 8, 2016, the Northern District of Illinois granted plaintiff's motion to unseal the case, revealing the plaintiff's legal theories and bringing the defendant's vulnerabilities to light. Memorandum Opinion and Order at 1, Shore v. Johnson and Bell, 2016 WL 7197421 (N.D. Ill. 2016) (No. 16-cv-4363).

[113] Complaint at 21–28, Shore v. Johnson and Bell, 2016 WL 7197421 (N.D. Ill. 2016) (No. 16-cv-4363).

[114] *Id.* at 28–29.

[115] Kat Greene, *NY Couple Says Attorney Negligent for Using AOL Email*, LAW360 (Apr. 18, 2016), http://www.law360.com/articles/786001/ny-couple-says-attorney-negligent-for-using-aol-email.

[116] *Id.*

Here, though, because the plaintiffs made the deposit and only recovered a portion of the funds, they can make a showing of actual damages.

As the number of hacking incidents increases, we will see more and more clients of high profile firms without a remedy for the firm's inability to maintain adequate data security. For example, just last year, both Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP suffered data breaches.[117] When consumer information is stolen from credit card companies or retail chains, victims can often show economic injury for identity theft or unreimbursed fraudulent purchases. But more often law firm data is targeted for information on mergers, patent and trade secrets or litigation strategy and does not cause traditional economic harm.[118] If our judicial system is to hold law firms accountable for out-of-date cybersecurity practices, we must create a right of action for private citizens negatively affected, though not necessarily traditionally economically injured, by data breaches.

## CONCLUSION

In conclusion, law firm data security is governed by state ethical obligations, state data breach notification laws, and minimally enforced by malpractice suits. There is no federal standard of regulation, so each individual state has had to create and interpret these rules. Because this is a new area of law for many courts and large corporations tend to settle cases before the litigation stage, legal precedent is not much help in evolving the doctrine to encompass new rights that follow technological trends. While a vague national standard that preempts state laws would be a step backward for consumer protection, a national standard would allow corporations and other entities to more easily comply with data security standards by eliminating individual nuances of state regulation in states where they conduct business. Massachusetts, for example, while in opposition to a national law that preempts its more rigorous state standards, is in favor of a law that would continue to require breach notification to state authorities who would ultimately be responsible for enforcement.[119]

Our legal system needs to focus more on preventative measures instead of only providing remedies after a breach has occurred, and often only when there has been a violation of a data breach notification statute or demonstrable damages. If we wait for each individual firm to get hacked before determining that its protection measures were inadequate, then more and more confidential client information will be exposed before the firm has any incentive to update their policies, especially if the only

---

[117] Randall & Kroll, s*upra* note 1, at 54.
[118] *Id.*
[119] Smoyer & Chow, *supra* note 6.

incentive is negative publicity rather than reparations to the injured parties or monetary penalties. Courts need to step up, like the court of the Northern District of California in *Adobe Systems*,[120] to interpret unauthorized access to data as creating a risk of imminent harm, rather than purely speculative harm. The legislature needs to step up and enact standard of care laws for data protection, giving individuals a private right of action to seek damages for businesses' failure to comply. The law has always been slow to catch up to technological advances, but leaving this regulatory gap unaddressed could come at a steep price.

[120] Even though the case ultimately settled without litigation of the substantive issues, precedents legitimizing data breaches as injury-in-fact for Article III standing could create a higher risk of litigation for organizations and incentivize more rigorous precautionary security measures.