ACCOUNTABILITY IS THE BEST (PRIVACY) POLICY: IMPROVING REMEDIES FOR DATA BREACH VICTIMS THROUGH RECOGNITION OF PRIVACY POLICIES AS ENFORCEABLE AGREEMENTS

Madelyn Tarr*

CITE AS: 3 GEO. L. TECH. REV. 162 (2018)

INTRODUCTION

Your personal information has already been stolen. Statistically speaking, that is.[1] From 2005 to 2017, 7,674 data breaches exposed over one billion U.S. consumer records.[2] While this statistic includes the eighty

* Duke University School of Law, J.D./LL.M in Law and Entrepreneurship, 2018. I would like to thank Professor Rebecca Rich and the members of her Fall 2017 Scholarly Writing Workshop for their invaluable guidance and feedback during the planning and drafting stages of this article.

[1] In Spring 2016, the Pew Research Center study found that 64% of Americans had experienced a breach of their personal information. Given this information, combined with the almost half of Americans' data compromised in the Equifax hack in 2017, it is more likely than not that an American's data has been breached. Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, PEW RESEARCH CTR. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity [https://perma.cc/R9TZ-CT5EDE2E-RW5J].

[2] Robert Farrington, *Calm Down! Your Identity Has Already Been Stolen*, THE COLL. INV'R (Sept. 14, 2017), https://thecollegeinvestor.com/20167/identity-stolen [https://perma.cc/V2WK-CNJG]. Global statistics are even more alarming. Over 4 billion records were stolen in 2016 in over 4000 hacking incidents. Herb Weisbaum, *More Than 4 Billion Data Records Were Stolen Globally in 2016*, NBC NEWS (Jan. 30, 2017, 7:31 AM), https://www.nbcnews.com/storyline/hacking-in-america/more-4-billion-data-records-were-stolen-globally-2016-n714066 [https://perma.cc/5G8Y-XEAN]. For further information, Breach Level Index presents a chilling real-time count of records stolen in data breaches worldwide as well as a detailed list of those security incidents. Data Breach Statistics, BREACH LEVEL INDEX, http://www.breachlevelindex.com [https://perma.cc/B8BY-72VH].

million Social Security numbers stolen in Anthem's 2015 hack,[3] it does not account for the 145.5 million Social Security numbers that were compromised in the 2017 Equifax hack.[4] These hacks are not idle threats to consumers: $16.8 billion was stolen from U.S. consumers through identity theft in 2017.[5]

The reality is that data storage on the Internet is more interconnected than ever. Hackers may only gain access to a person's email address and password—a problem with a seemingly simple solution: just change the password. But those hackers may have gained access to more than someone's innocent email conversations. One survey estimates that thirty-five percent of adults keep sensitive medical and financial information in their email, including bank statements, tax returns, and health records.[6] A significant percentage of adults also store loan and mortgage information, pin numbers and passwords, and other personal records both in their email accounts and through cloud-based storage platforms, like Dropbox and Google Drive.[7] These accounts, once compromised, can be a treasure trove of data for hackers, warranting years of credit monitoring, cancellation, and reestablishment of accounts, often causing anxiety for victims.[8]

Yet courts presented with data breach claims still assert that "plaintiffs do not explain how the stolen data would be used to perpetrate

---

[3] In 2015, health insurance company Anthem suffered a data breach of 80 million customer records. Farrington, *supra* note 2.

[4] *Id.* Nor does this statistic include the recent estimates by Yahoo that 3 billion user accounts, rather than its earlier estimates of 1 billion, were compromised in the company's 2013 data breach. Lily Hay Newman, *Yahoo's 2013 Email Hack Actually Compromised Three Billion Accounts*, WIRED (Oct. 3, 2017, 7:29 PM), https://www.wired.com/story/yahoo-breach-three-billion-accounts [https://perma.cc/86CG-UUTR].

[5] *Facts and Statistics: Identity Theft and Cybercrime*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime [https://perma.cc/R4RB-252C].

[6] LexisNexis Risk Solutions, *LexisNexis Risk Solutions-Sponsored Survey Finds More Than One-Third of Americans Store Tax, Bank, Health and Other Sensitive Records in Email, Cloud and Electronic Systems*, PR NEWSWIRE (Oct. 3, 2016), https://www.prnewswire.com/news-releases/lexisnexis-risk-solutions-sponsored-survey-finds-more-than-one-third-of-americans-store-tax-bank-health-and-other-sensitive-records-in-email-cloud-and-electronic-systems-300338041.html [https://perma.cc/8PK3-HBRL].

[7] *Id.*

[8] *See* Adam Shell, *Equifax Data Breach Could Create Lifelong Identity Theft Threat*, USA TODAY (Sept. 9, 2017), https://www.usatoday.com/story/money/2017/09/09/equifax-data-breach-could-create-life-long-identity-theft-threat/646765001 [https://perma.cc/UB8C-9XVK].

identity theft"[9] or "[a]ppellants have alleged no misuse, and therefore, no injury."[10] Similarly, courts have been disinclined to accept that hackers can cause damage with nontraditional identifying information: "[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."[11] The U.S. judicial system has yet to reconcile the threat of data theft with the reality of its compounding impact.

When someone's identity is stolen and used to make fraudulent purchases or to open new accounts, there is often no legal recognition of economic injury—credit card companies will waive fraudulent charges and closure of falsified accounts is costless. However, victims must sacrifice valuable time they could have spent on work, family, education, and other life experiences to deal with the aftermath of identity theft and complete tasks such as closing existing online and financial accounts.[12] A 2015 report focusing on the emotional impact of identity theft, promulgated by the recent data breach expert, Equifax, stated that victims often experience similar emotions as trauma survivors, such as feelings of vulnerability and isolation, in addition to suffering from financial stress.[13] Increased awareness and monitoring of accounts is necessary for years following the initial identity theft incident. Without "real" economic injury and no proof of future risk of misuse of personally identifiable information (PII),[14] victims often have no recourse against hackers who are

[9] *In re* VTech Data Breach Litig., No. 15 CV 10889, 2017 WL 2880102, at *4 (N.D. Ill. July 5, 2017) (refusing to confer standing, the court stated that the stolen information, including VTech usernames, passwords, birthdates, secret questions, and other account information, could not be used to open a credit card or other bank account so therefore it could not be used for identity theft).

[10] Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3d Cir. 2011) (reasoning that without actual misuse of the breached data, because there was no evidence that the data breach was "intentional or malicious" or that hackers intended to misuse the information, the plaintiff had not shown injury).

[11] Antman v. Uber Techs., Inc., No. 3:15-cv-01175-LB, 2015 WL 6123054, at *10–11 (N.D. Cal. Oct. 19, 2015) (explaining that because the only data that had been stolen in Uber's breach was names and driver's license numbers, there was no risk that the information could be misused to cause the injury necessary to confer standing).

[12] IDENTITY THEFT RES. CTR., IDENTITY THEFT: THE AFTERMATH 11 (2016), https://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf [https://perma.cc/XPW2-J8NH].

[13] *See A Lasting Impact: The Emotional Toll of Identity Theft*, EQUIFAX (Feb. 2015), https://www.equifax.com/assets/PSOL/15-9814_psol_emotionalToll_wp.pdf [https://perma.cc/54YY-E57F].

[14] On a broad level, PII "refers to information that can be used to identify, locate, or contact an individual, alone or when combined with other personal or identifying information." *Personal Information*, PRACTICAL LAW GLOSSARY ITEM 1-501-8805

frustratingly impossible to track or against the companies which enable those hackers with lax security policies.[15]

Consumers need a reliable remedy. Current data protection infrastructure effectively leaves consumers without recourse in the event their information is improperly accessed and stolen during a hacking incident. The solution is seemingly simple: a federal statute that (1) requires businesses that collect consumer data to comply with standardized security measures and (2) grants victims of hacks that result from noncompliance a private right of action.[16] Yet, given the political climate and the fate of recent privacy regulation proposals, enactment of such a law is far from simple.[17] In March 2017, Congress overturned rules that would have increased privacy protections for consumers through the regulation of Internet service providers (ISPs); President Trump approved this action in April.[18] This willingness to strike down regulation that would limit how ISP giants such as Verizon, Comcast, and AT&T could use consumer data suggests a political trend toward business-friendly policies at the expense of consumer privacy protection.[19] The White

(2018). Specific definitions of PII as well as what types of information is included in the definition vary based on applicable state and federal law. For example, California includes name, address, email address, telephone number, Social Security number and any other contact information in its definition of PII. CALIF. BUS. & PROF. CODE § 22577. Massachusetts defines PII as name combined with any of the following: Social Security number, driver's license number, and any financial account information. 201 MASS. CODE. REG. 17.02.

[15] A recent survey of executives worldwide showed that 44% of companies do not have an overall information security strategy and 54% do not have an incident response process. PWC, STRENGTHENING DIGITAL SOCIETY AGAINST CYBER SHOCKS: KEY FINDINGS FROM THE GLOBAL STATE OF INFORMATION SECURITY SURVEY 2018 4 (2017), https://www.pwc.com/us/en/cybersecurity/assets/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf [https://perma.cc/3X4L-X6PY].

[16] *See*, *e.g.*, Alec Wheatley, *Do-It-Yourself Privacy: The Need For Comprehensive Federal Privacy Legislation with a Private Right of Action*, 45 GOLDEN GATE U. L. REV. 265, 283–84 (2015); Patricia Cave, Comment, *Giving Consumers a Leg to Stand On: Finding Plaintiffs a Legislative Solution to the Barrier From Federal Courts In*, 62 CATH. U. L. REV. 765, 789–94 (2013).

[17] *See* discussion *infra* Part I on recent privacy legislation proposals.

[18] Kimberly Kindy, *How Congress Dismantled Federal Internet Privacy Rules*, WASH. POST (May 30, 2017), https://www.washingtonpost.com/politics/how-congress-dismantled-federal-internet-privacy-rules/2017/05/29/7ad06e14-2f5b-11e7-8674-437ddb6e813e_story.html [https://perma.cc/FC3F-4WZN]. *See infra* Section I.d for further discussion of the ISP rules.

[19] *See* David Cowan, *How a Trump Presidency Will Erode Cyber Privacy and National Security*, FORBES (Nov. 30, 2016), https://www.forbes.com/sites/valleyvoices/2016/11/30/how-a-trump-presidency-will-erode-cyber-privacy-and-national-security/#5ffcc277584e [https://perma.cc/PZ5M-BHWU]; Brian Fung, *House Sends Bill Rolling Back Internet Privacy Protections to Trump*, WASH. POST (Mar. 28, 2017),

House is working with companies like Facebook and Google to draft federal privacy regulation,[20] though the drafting process could take years and result in lenient, company-favorable policies.

Because any proposed federal regulation could be years away and still must receive Congress's stamp of approval, courts should turn to the contractual nature of the privacy policies consumers agree to when accessing an online service. Most companies require consumers to agree to a privacy policy concurrently with a terms of use agreement when signing up for an online service. The terms of use agreement, when presented in clickwrap form, is considered by courts to be an enforceable agreement.[21] However, historically, courts have been less than enthusiastic about relying on the language of privacy policies (which companies often do not intend to be a binding agreement) as a promise to consumers to maintain a certain standard of data safeguards.[22] Moreover, courts often are reluctant to assign value to PII, stifling claims before the merits of the argument are litigated.[23]

This article proposes that courts should begin to consistently recognize a threat of future identity theft as injury-in-fact for Article III standing[24] with mitigation expenses, overpayment for services, and loss of

---

https://www.washingtonpost.com/business/economy/house-sends-bill-rolling-back-internet-privacy-protections-to-trump/2017/03/28/db704ca4-13d5-11e7-9e4f-09aa75d3ec57_story.html [https://perma.cc/3F3R-94SL].

[20] David Shepardson, *Trump Administration Working on Consumer Data Privacy Policy,* REUTERS (July 27, 2018), https://www.reuters.com/article/us-usa-internet-privacy/trump-administration-working-on-consumer-data-privacy-policy-idUSKBN1KH2MK [https://perma.cc/HMQ8-XKVT]; Tony Romm, *The Trump Administration Is Talking to Facebook and Google About Potential Rules for Online Privacy*, WASH. POST (July 27, 2018), https://www.washingtonpost.com/technology/2018/07/27/trump-administration-is-working-new-proposal-protect-online-privacy/ [https://perma.cc/KV27-SCGZ].

[21] Clickwrap agreements are enforceable online agreements where "users are 'required to click on an "I agree" box'; they must expressly manifest assent to the terms and conditions." *In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1165 (N.D. Cal. 2016) (citing Nguyen v. Barnes & Noble Inc., 763 F.3d 1171, 1175–76 (9th Cir. 2014)). For an online agreement to be enforceable, the dispositive question is "whether the website puts a reasonably prudent user on inquiry notice of the terms of the contract." *Nguyen*, 763 F.3d at 1177. *See also infra* Section III.b.i.

[22] Thomas B. Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 181, 190–95 (2016); *see, e.g.*, Jurin v. Google Inc., 768 F. Supp. 2d 1064, 1073 (E.D. Cal. 2011); Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1199–200 (D.N.D. 2004); *In re* Nw. Airlines Privacy Litig., No. Civ. 04-126(PAM/JSM), 2004 WL 1278459, at *4–5 (D. Minn. June 6, 2004).

[23] Norton, *supra* note 22, at 193–94.

[24] Class action suits most often result from data breaches and therefore common law claims such as negligence and breach of contract are tried in federal courts with a constitutional standing requirement rather than state courts. Daniel Bugni, *Standing*

value of PII as economic injury.[25] The reality of hacking is that misuse of improperly-accessed information is a credible risk requiring affected parties to spend time, energy, and money on preventative or remedial measures to mitigate the threat of identity theft. Privacy policies that consumers agree to in conjunction with companies' binding terms of service should be considered enforceable agreements; language claiming the company will use "reasonable standards" of security or "industry-standard safeguards" should be considered definite enough for a breach of contract claim. Holding companies accountable for lax security practices and giving hacking victims more than a laughable opportunity for a legal remedy should be a priority for courts.[26]

This solution is not all encompassing nor is it immune to loopholes and sidestepping. But until Congress is ready for a commitment to privacy regulation, the judicial system must proactively begin to set the stage for recognition of data security as an essential business practice with an undeniable impact on consumers. This does not mean to suggest that courts should circumvent Congress to create their own rules; instead, courts should shift their reasoning to match circuits that have already begun to recognize tangible damage to consumers and should extend parallel reasoning to both terms of use agreements and privacy policies.

Part I will introduce the existing (and fragmented) statutory regulation of data security at both the federal and state levels. Federal law

---

Together: An Analysis of the Injury Requirement in Data Breach Class Actions, 52 GONZ. L. REV. 59, 61–62 (2017).

[25] Recent data breach litigation suggests that courts are more and more willing to accept privacy policy-based breach of contract claims with damages such as overpayment, loss of sales value of PII, and mitigation expenses. *See*, *e.g.*, *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783, at *12–16 (N.D. Cal. May 27, 2016) (overpayment, loss of value of PII, and mitigation expenses); Kuhns v. Scottrade, 868 F.3d 711, 716 (8th Cir. 2017) (overpayment); *In re* VTech Data Breach Litigation, No. 15 CV 10889, 2017 WL 2880102, at *5 (N.D. Ill. July 5, 2017) (overpayment).

[26] A Ninth Circuit case, *In re* Zappos.com, Inc., with a petition for certiorari is pending before the Supreme Court as of the writing of this paper. The controversy directly addresses the existing circuit split regarding Article III standing in data breach cases. A decision in this case would greatly affect consumer success in data breach lawsuits by either facilitating the progression of consumer claims or rendering it impossible for consumers to show standing, barring other intervening legal developments. However, given that the Court recently denied certiorari to *Attias v. Carefirst*, which similarly addressed this issue, it is unclear whether the Court will hear the case. *In re* Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018), *petition for cert. filed*, No. 18-225 (Aug. 20, 2018); *see also* Hanley Chew & Tyler G. Newby, *Appellate Court Finds Risk of Identity Theft Sufficient to Establish Standing, Circuit Split Worsens*, FENWICK & WEST LLP (Mar. 9, 2018), https://www.fenwick.com/publications/Pages/Appellate-Court-Finds-Risk-of-Identity-Theft-Sufficient-to-Establish-Standing-Circuit-Split-Worsens.aspx [https://perma.cc/49KR-UJXU].

would be an ideal solution to the inadequacies of the current system, but the bleak future of federal privacy regulation and standardization of data security practices makes this goal overly idealistic and impractical. Part II will continue this introduction, focusing on potential common law claims that affected consumers can bring after their personal information is stolen in a data breach. These claims have been historically unsuccessful in court, often due to the court's refusal to recognize the risk of misuse of personal information as an injury-in-fact necessary to confer the requisite Article III standing. Part III proposes a more practical solution for the lack of remedies for consumers: data privacy should be regulated through validation of companies' privacy policies as binding agreements. This solution would be a more realistic (although an imperfect and temporary) means of holding companies accountable for a data breach until a more comprehensive federal law is enacted.

I. STATUTORY REGULATION OF DATA SECURITY

Currently, despite many attempts at enactment,[27] no comprehensive federal data security regulation exists.[28] That means barring state laws, nothing regulates whether the average company must implement data security measures to protect the mountain of information it collects and maintains on its users.[29] And nothing requires these

[27] Between 2005 and 2011, numerous federal privacy regulation bills were proposed but none were passed by Congress. When the FTC and the White House called for privacy reform in 2012, the highly partisan Congress was unable to execute; Republicans were determined to stop regulation in its tracks, citing onerous requirements on businesses as a threat to the economy. When President Obama released a draft privacy bill in 2015, the laws reflected an attempt to accommodate Republican concerns on over-regulation, but the bill was criticized for the weak level of protection it provided. Many perceived the legislation as dead on arrival. It did not pass. Cave, *supra* note 16, at 767, n. 14; Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 360–61 (2015).

[28] *See* sources cited *supra* note 20.

[29] It is worth noting that the newly effective General Data Protection Regulation (GDPR) regulates companies, wherever located, that store data on European Union residents. Many U.S. companies have updated their privacy protocols to comply with this heightened standard. While it does require that companies processing data of EU residents maintain reasonable security measures to protect the data, "reasonable" is undefined and open to interpretation. The regulation doesn't affect all U.S. companies, only the EU can penalize for noncompliance with fines, and the regulation gives no legal protection to U.S. residents. Companies may improve their data storage protections overall, giving U.S. residents the benefit of the law, but no legal redress. *See generally* Regulation (EU) 2016/679. *See also* Michael Nadeau, *General Data Protection Regulation (GDPR): What You Need to Know to Stay Compliant*, CSO (Apr. 23, 2018), https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html [https://perma.cc/MVD7-G8RE].

companies to disclose to users how they actually secure data. Fragmented statutory coverage regulates certain sectors of the economy and the collection of information about specific subgroups of people, but none of these regulations provide any protection for an adult consumer using the online services of an average commercial entity.

This section gives an overview of the existing fragmented federal and state data privacy regulation, demonstrating why the United States' current privacy infrastructure is inadequate to protect the average consumer interacting on the Internet with a business entity.

A. Existing Federal Regulation

The federal regulation that does exist is fragmented into different sectors, regulating entities that store healthcare data,[30] educational data,[31] financial data,[32] and any data belonging to children.[33] Broadly, these statutes set privacy standards and require implementation of safeguards to protect data that fall into the specified sectors. The regulation in those areas could explain why businesses in unregulated industries have accounted for the highest percentage of breaches of any industry.[34] Since 2005, the business sector accounted for 45.2% of the overall number of reported breaches.[35] The healthcare/medical industry accounted for 34.5%, education accounted for 9%, government and military accounted for 6.6%, and banking/credit/financial breaches accounted for 4.8%.[36] These statutes require compliance by specific groups and entities that fall under the purview of the law and all, but one, leave individuals without a right of action. For a broad overview of the type of information storage that these laws regulate, see the chart in Appendix A.

Overall, these sectoral statutes regulate the maintenance of personal information that is traditionally considered more sensitive than

---

[30] *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA) P.L. No. 104-191, 110 Stat. 1936.

[31] *See* Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (2018).

[32] *See* Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681c-1; Gramm–Leach–Bliley Act (GLBA) P.L. 106-102, 113 Stat. 1338 (1999).

[33] *See* Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 (2018).

[34] Correlation is not causation, but this data might suggest that either unregulated businesses have lower data security standards making them attractive targets for hackers, or that other industries may be targeted at the same rate, but businesses suffer data breaches more often because they tend to have more lax security measures.

[35] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and Cyberscout*, IDENTITY THEFT RES. CTR. (Jan. 19, 2017), https://www.idtheftcenter.org/2016databreaches [https://perma.cc/NHR7-CUMT].

[36] *Id.* This data was compiled in January 2017 and does not include any breaches that occurred more recently than that.

that of the average consumer making an online purchase. But despite the enhanced data protection requirements, consumers still lack the right to sue for damages in cases of noncompliance.

B. Existing State Regulation

States similarly lack comprehensive data privacy regulation. Certain states, like Massachusetts and California, have made cybersecurity a priority by enacting laws[37] mandating higher standards of security practices among businesses than most other states require.[38] Despite a push for state legislation in 2017 after Congress overturned rules that would have regulated ISPs, it appears that many states may only minimally increase protection.

1. Data Breach Notification Laws

Every state has a data breach notification statute requiring companies and other entities that have suffered a data breach incident to notify individuals whose PII has been compromised.[39] While the core substance of the laws—that a regulated entity must notify consumers when their data has been improperly accessed—is universal among the states, the statutes vary widely on the definition of PII, the definition of a breach, notification requirements, and which entities fall under the purview of the rule. [40] A universal data breach notification statute modeled after state law is the most likely candidate for successful federal privacy regulation and would create a baseline for further comprehensive privacy protections.[41] However, even though data breach notification is widely accepted as a necessary consumer protection, past attempts to enact a notification statute have proven unsuccessful in garnering the consensus necessary for enactment by Congress.[42]

---

[37] 201 MASS. CODE REGS. 17.01–05 (2018); CAL. CIV. CODE § 1798.81.5(b) (2016).

[38] *See* Corey M. Dennis, *Data Security Laws and the Rising Cybersecurity Debate*, LEXOLOGY (Jan. 28, 2013), https://www.lexology.com/library/detail.aspx?g=cc5c9a56-7a60-46ab-9cf4-f36cada0cafa [https://perma.cc/H358-G4D2].

[39] *See Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGS. (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/33DQ-TFJV].

[40] *Id.*

[41] Cory Bennett, *Lawmakers See Momentum for Data Breach Legislation*, THE HILL (Jan. 27, 2015, 12:34 PM), http://thehill.com/policy/cybersecurity/230867-data-breach-bill-is-achievable-goal [https://perma.cc/7QEG-6PYV].

[42] *Id.* In 2015, as the number of data breach incidents began to escalate, many observers believed that a comprehensive data breach notification statute would be the most likely privacy legislation to pass. Congress agreed, seeing data breach as an important topic to

In addition, as models for a federal privacy statute, the state statutes are subpar with regard to the consumer protections they provide. While they do take the first step in holding companies accountable to the public, state data breach notification statutes have two major downfalls: they are remedial rather than preventative, and most do not provide a private right of action to individuals for violations.[43] In other words, the statutes only become relevant after a breach has occurred, and companies are merely subject to civil penalties if they fail to notify consumers about the breach in accordance with the law's requirements.[44] Only eleven states give consumers the ability to seek redress for the consequences of untimely or improper notification;[45] courts in those states have been reluctant to find that consumers are injured by late notification.[46] Overall, these laws do not incentivize companies to adequately protect their data.

2. Other State Laws

Even some states in favor of privacy regulation have shown opposition to the idea of a comprehensive federal law and have preferred to focus regulation efforts at the state level. The Massachusetts Attorney General in 2016 was vocal in her opposition to federal privacy legislation, arguing that federal legislation would provide weak protection and preempt the stricter standards that Massachusetts specifically placed in its state laws.[47] Other states that have carefully enacted data privacy laws

---

address in the form of a statute uniting the fragmented forty-seven state data breach notification laws. But even a law that most states and Congress already recognized as necessary was unable to advance. Brookman, *supra* note 28, at 360–61; Bennett, *supra* note 41.

[43] *See generally* MINTZ LEVIN, STATE DATA SECURITY BREACH NOTIFICATION LAWS (2018), https://www.mintz.com/sites/default/files/media/documents/2018-09-18/UPDATED%20State%20Data%20Breach%20Matrix%20June%202018.pdf [https://perma.cc/HP28-NCVH].

[44] *Id.*

[45] Those states are Alaska, California, Louisiana, Maryland, New Hampshire, North Carolina, South Carolina Tennessee, Virginia, Washington, and potentially Massachusetts. *Id.* ("If Attorney General finds violation of consumer protection laws for unfair or deceptive acts or practices, Massachusetts consumers may seek damages under Chapter 93A.").

[46] *See, e.g.*, Corona v. Sony Pictures Ent., Inc., No. 14-CV-09600 RGK, 2015 WL 3916744, at *9 (C.D. Cal. June 15, 2015); Dugas v. Starwood Hotels & Resorts Worldwide, Inc., No. 3:16-cv-00014-GPC-BLM, 2016 WL 6523428, at *6 (S.D. Cal. Nov. 3, 2016); *In re* Sony Gaming Networks & Customer Data Security, 996 F. Supp. 2d 942, 965 (S.D. Cal. 2014).

[47] Divonne Smoyer & Kimberly Chow, *Q&A with Massachusetts AG Maura Healey*, INT'L ASS'N OF PRIVACY PROF'LS (Aug. 23, 2016), https://iapp.org/news/a/qa-with-massachusetts-ag-maura-healy [https://perma.cc/C2TB-NX9N].

may demonstrate similar opposition to a federal law that weakens their residents' protections.

California, known for its presence at the forefront of technological and legal advances, enacted a statute, effective in 2015, requiring businesses to maintain "reasonable security practices" when storing the information of a California resident.[48] Along with Massachusetts, California is one of the minority of states to have created an information standard of care statute.[49] The Massachusetts statute, effective in 2010, accurately reflects the state's goal of maintaining the most stringent cybersecurity regulations in the country—the law requires anyone who owns or licenses personal information about a Massachusetts resident to adopt a comprehensive information security program.[50]

The Massachusetts statute is enforceable only by the state's Attorney General, while the California law allows a more progressive enforcement mechanism: private actions.[51] State enforcement of the Massachusetts law only provides injunctive relief or civil penalties, without passing relief on to consumers, similar to most of other state statutes.[52] Yet, despite California's attempt to offer data breach victims a chance at redress, plaintiffs face the same Article III standing obstacles as common law claims.[53] California district courts have handed down more favorable decisions on standing than the rest of the country, but plaintiffs still face resistance at the standing stage and in subsequently convincing the court to rule in the plaintiff's favor and award damages.

As a response to an uptick in data privacy scandals,[54] California enacted the California Consumer Privacy Act in July 2018, effective on

---

[48] CAL. CIV. CODE § 1798.81.5(b) (2016) ("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.").

[49] As of October 2018, twenty-two states have laws requiring individuals or businesses maintaining personal information to use reasonable procedures to safeguard data. *Data Security Laws—Private Sector*, NAT'L CONF. OF STATE LEGS. (Oct. 15, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx [https://perma.cc/FL2A-74D8].

[50] 201 MASS. CODE. REGS. 17.01–05 (2018); Smoyer & Chow, *supra* note 47.

[51] CAL. CIV. CODE § 1798.84(b) (2010); MASS. GEN. LAWS ANN. ch. 93H, § 6 (West 2018).

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

[53] *See infra* Section II.a.

[54] One such example is the Facebook-Cambridge Analytica incident, in which a political data firm gained access to over 50 million Facebook users' private information through an unauthorized transfer of data. *See generally* Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 18,

January 1, 2020, providing California residents with new protections regarding use of their PII.[55] The law expands the definition of PII and gives California residents (1) the right to know what PII entities are collecting and for what purpose, (2) the right to access a copy of the PII collected from them, (3) the right to request deletion of their PII, (4) the right to opt out of the sale of their PII, and (5) freedom from discrimination by the entity for exercising the above-mentioned rights.[56] These rights are solely enforced by the California Attorney General; however, the act creates a private right of action for data breach victims whose PII was improperly accessed due to a failure to maintain reasonable security practices.[57] This statute is a leap forward in data privacy regulation because of its likely effects on businesses beyond their interactions with California residents.[58] However, regardless of the spillover benefits other state residents may receive, only California residents' rights are protected under statutory authority. There is still a time gap until the law becomes effective, so the ultimate effects of this law are unknown.

Many states use unfair or deceptive business practices laws that parallel the Federal Trade Commission (FTC) Act,[59] aptly nicknamed mini-FTC laws, to prosecute data breach targets.[60] Most well-known is California's Unfair Competition Law, which the state's Attorney General, similar to the FTC, has used as an authority to prosecute companies with unreasonable security measures.[61] Individuals can have standing under the law as long as they can prove injury-in-fact and have lost money or property from the data breach.[62] As an equitable action, remedies under the law are limited to restitution and injunctive relief.[63] States like Connecticut, Pennsylvania, and Florida enforce noncompliance of their

---

2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [https://perma.cc/8BEP-EU5N].

[55] *See* CAL. CIV. CODE § 1798.100 (2018).

[56] *Id*. §§ 1798.100–25.

[57] *Id.* § 1798.150.

[58] These broad effects may be similar to those produced by CalOPPA's privacy policy requirement. *See infra* Section I.b.iii.

[59] *See infra* Section I.c. for a discussion of the FTC's authority under the Act.

[60] Evan M. Wooten*, The State of Data Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 229, 231 (2015).

[61] CAL. BUS. & PROF. CODE § 17200 (2018); Kathryn F. Russo, *Regulation of Companies' Data Security Practices Under the FTC Act and California Unfair Competition Law*, 23 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 201, 207–08 (2014).

[62] Pom Wonderful LLC v. Welch Foods, Inc., No. CV 09-567 AHM (AGRx), 2009 WL 5184422, at *2 (C.D. Cal. Dec. 21, 2009).

[63] *Id.*

data breach notification statutes as unfair or deceptive trade practices, but the statutes are exclusively enforced by their respective Attorney Generals.[64]

3. CalOPPA and DOPPA

A few states have recently begun to regulate the privacy policies and notices of companies that collect or maintain data on their residents.[65] California, as expected, was the first to enact such a law in 2013, as an amendment to the California Online Privacy Protection Act ("CalOPPA"). For three years it was the sole regulator of privacy policies and quite possibly the only reason why many companies make their policies accessible to users. [66] Delaware followed suit in 2016 with the Delaware Online Privacy Protection Act ("DOPPA"), similarly regulating privacy policy presentation.[67] In 2017, Nevada stepped into the ring, creating its own regulation on privacy policies.[68] The following chart highlights the similarities and differences between the three statutes that require covered persons to make privacy notices available to consumers.

Statute	Coverage	Notice Requirements	Content of Privacy Policies
CalOPPA[69]	Any person who collects or maintains data on	Notice must be "conspicuously post[ed]."	Must (1) identify categories of PII that the operator collects, (2) describe the process (if any) to review and change

[64] CONN. GEN. STAT. ANN. § 36a-701b(g) (West 2018); 73 PA. STAT. AND CONS. STAT. ANN. §§ 2301–2308, 2329 (West 2018); FLA. STAT. ANN. § 501.171 (West 2018); *see also* BAKERHOSTETLER, STATE DATA BREACH LAW SUMMARY 12, 16, 76 (2017), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_FFor.pdf [https://perma.cc/M7U8-GUCN].

[65] These states include California, Delaware, and Nevada. Connecticut has a similar, albeit limited, statute requiring companies that collect Social Security numbers to publicly display a privacy policy meeting certain confidentiality requirements. *State Laws Related to Internet Privacy*, NAT'L CONF. OF STATE LEGS. (June 20, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx [https://perma.cc/EFZ7-MA2Q].

[66] *The Top Three Privacy Takeaways of the New Delaware Online Privacy and Protection Act*, BRYAN CAVE (April 3, 2016), https://www.bryancave.com/en/thought-leadership/the-top-three-privacy-takeaways-of-the-new-delaware-online.html [https://perma.cc/7FLE-QCRS].

[67] DEL. CODE ANN. TIT. 6, § 1205C (West 2018).

[68] *State Laws Related to Internet Privacy*, *supra* note 65.

[69] CAL. BUS. & PROF. CODE §§ 22575–78 (West 2018).

	California residents		a user's PII, (3) describe the notification process for material changes to the policy, (4) identify the policy's effective date, (5) disclose the operator's response to "do not track" signals, and (6) disclose third-party rights to collect PII about a user's online activities.
DOPPA[70]	Any person who collects or maintains data on Delaware residents	Notice must be "conspicuously available"; enumerates specific ways to conspicuously display the notice.	Must (1) identify categories of PII that the operator collects, (2) describe the process (if any) to review and change a user's PII, (3) describe the notification process for material changes to the policy, (4) identify the effective date, (5) disclose the operator's response to "do not track" signals, and (6) disclose third-party rights to collect PII about a user's online activities.
Nevada S.B. 538[71]	Any person who collects or maintains data on Nevada residents	"[A]n operator shall make [its privacy policy] available, in a manner reasonably calculated to be accessible by consumers whose covered information the	Must (1) identify categories of PII that the operator collects, (2) describe the process (if any) to review and change a user's PII, (3) describe the notification process for material changes to the policy, (4) disclose third-party rights to collect PII about a user's online

[70] DEL. CODE ANN. TIT. 6, § 1205C (West 2018).
[71] NEV. REV. STAT. ANN. § 603A (West 2018).

		operator collects."	activities, and (5) identify the effective date; waives requirement to post a privacy policy if the operator resides in-state, Internet sales are a minority of the operator's income, or the site has below 20,000 visitors per year.

The statutes, while lacking any requirements for disclosure of security practices, do provide an essential benefit to consumers country-wide. The statutes reach any businesses that store the PII of California, Delaware, or Nevada residents, and with the high likelihood that a company doing business online will transact with residents of those states, the laws effectively require all online businesses to post a privacy policy. However, the information required to be placed in the policies is minimally protective. Consumers are now aware (assuming careful scrutiny of the text, of course) of the types of data companies collect and what they can do with the data. But sharing any information on how PII is protected or the privacy safeguards the company employs is completely discretionary. Without any legal standard of disclosure, privacy policies often use vague language to describe how they protect data, placating consumers with assurances of the utmost commitment to data privacy.[72] Thus, these laws provide no way for consumers to hold companies accountable for lax data security standards.

C. Federal Trade Commission Enforcement Authority

The FTC plays a substantial role in penalizing data breach targets by using its enforcement authority under Section 5 of the FTC Act, which

[72] *See, e.g.*, *Privacy Policy*, WALT DISNEY CO. (May 9, 2018), https://privacy.thewaltdisneycompany.com/en/current-privacy-policy/#heading8 [https://perma.cc/VEY2-4TLV] ("The security, integrity, and confidentiality of your information are extremely important to us."); *CBS Privacy Policy*, CBS INTERACTIVE (Apr. 23, 2018), https://www.cbsinteractive.com/legal/cbsi/privacy-policy [https://perma.cc/U4AS-6SJ4] ("We are committed to protecting your information."); *Spotify Privacy Policy*, SPOTIFY, (May 25, 2018), https://www.spotify.com/us/legal/privacy-policy/#s1 [https://perma.cc/V645-CYJR] ("We are committed to protecting our users' personal data.").

prohibits unfair or deceptive trade practices.[73] Section 5 has been used as a catch-all for imposing penalties on companies whose lax security standards allow hackers to wreak havoc on unsuspecting consumers.[74] Despite facing criticism for failing to publish guidance on unfair or deceptive data security practices, the FTC has continued to file complaints against companies that violate the law by misleading consumers about their data protection practices.[75] Most often, these suits end in settlements rather than litigation, though the FTC's authority in this arena may be dwindling.[76] The settlements call for various penalties and actions to be taken by the infringing companies, generally tailored to the specific incident—in past cases, the FTC has required implementation and evaluation of an information security program, payment of civil penalties, and restitution for consumer-victims.[77]

For example, when AshleyMadison.com was hacked in 2015, exposing thirty-six million user accounts as a result of deception and failure to properly protect user data, the company's settlement with the FTC required implementation of a comprehensive data security program as well as $1.6 million payment to settle FTC and state law claims.[78] In

---

[73] Paul R. Gaus, *Only The Good Regulations Die Young: Recognizing the Consumer Benefits of the FCC's Now-Defunct Privacy Regulations*, 18 MINN. J.L. SCI. & TECH. 713, 721 (2017); 15 U.S.C. § 45 (2006).

[74] *See* Wooten, *supra* note 60, at 236 ("The FTCA does not specifically empower the FTC to investigate, regulate, or seek enforcement regarding data security, but the FTC has assumed authority in this and other privacy and technology-related fields. . . .").

[75] *Id.*; Jimmy H. Koo, *Judges Question FTC Data Security Standard at LabMD Argument*, BLOOMBERG LAW (June 23, 2017), https://www.bna.com/judges-question-ftc-n73014460645 [https://perma.cc/7NEK-KRXQ]; *see also* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 616 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

[76] Wooten, *supra* note 60, at 236. The Eleventh Circuit's June 2018 decision in *LabMD, Inc. v. FTC* shows that the FTC's settlement authority may be weakening. The FTC had imposed an enforcement order on LabMD, requiring the company to overhaul its data security program after confidential patient data was made public. On appeal, the Eleventh Circuit held that the order was unenforceable because it "commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness." As the FTC has mandated data security system overhauls as one of its main enforcement mechanisms for years, other companies that have received such orders and companies receiving them in the future may challenge the FTC's authority. It is unclear whether this decision will have broad effect outside of the Eleventh Circuit. LabMD, Inc. v. FTC, 894 F.3d 1221, 1236 (11th Cir. 2018); *see also Eleventh Circuit LabMD Decision Significantly Restrains FTC's Remedial Powers in Data Security and Privacy Actions*, WILSON SONSINI GOODRICH & ROSATI (June 18, 2018), https://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-LabMD.htm [https://perma.cc/T2TW-3S2U].

[77] Wooten, *supra* note 60, at 235–36.

[78] Users of the website were assured that their data was protected by standards much higher than it actually was. The company had "no written information security policy, no

August 2017, Uber settled with the FTC after failing to monitor employee access to customer data and failing to secure customer data with reasonable security measures.[79] The settlement requires Uber to implement a comprehensive privacy program and receive independent third-party audits of its privacy protocols for the next twenty years.[80] These two examples, like many FTC settlements, penalize infringing companies but do nothing to redress consumer injury.

While these enforcement actions offer protection to consumers in the form of newly fortified security practices required by the FTC settlement, such enforcement only becomes relevant once a company's deceptive practices are exposed in a hacking incident. There are no legally binding security standards on companies other than a common sense standard: do not lie to your customers about your security practices. Because of the challenges of discretionary enforcement, the FTC has called for comprehensive privacy regulation reform.[81]

Its efforts have not been met with success. The FTC currently promulgates a Notice and Choice framework to be used as a guideline when representing data privacy standards to consumers.[82] In 1998, the FTC published a report outlining Fair Information Practice Principles that reflect the results of a study on widely-accepted information practices and reasonable safeguards among existing entities.[83] The principles are Notice, Choice, Access, Integrity, and Enforcement, with Notice and Choice as the

---

reasonable access controls, inadequate security training of employees, no knowledge of whether third-party service providers were using reasonable security measures, and no measures to monitor the effectiveness of their system security." Press Release, FTC, Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information (Dec. 14, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting [https://perma.cc/LHC2-HEPK].

[79] "Uber did not require engineers and programmers to use distinct access keys to access personal information stored in the cloud. Instead, Uber allowed them to use a single key that gave them full administrative access to all the data, and did not require multi-factor authentication for accessing the data. In addition, Uber stored sensitive consumer information, including geolocation information, in plain readable text in database back-ups stored in the cloud." Press Release, FTC, Uber Settles FTC Allegations that it Made Deceptive Privacy and Data Security Claims (Aug. 15, 2017), https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data [https://perma.cc/RP8X-M7QV].

[80] *Id.*

[81] FTC, PRIVACY ONLINE: FAIR INFO. PRACS. IN THE ELECTRONIC MARKETPLACE: A REP. TO CONGRESS 36–37 (2000) [hereinafter *Privacy Online*]; FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUS. AND POLICYMAKERS iv–v (2012), [hereinafter *Protecting Consumer Privacy*].

[82] *Privacy Online*, *supra* note 81; *Protecting Consumer Privacy*, *supra* note 81.

[83] FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998).

most prevalent standards.[84] The FTC's Notice and Choice guidelines recommend that companies self-regulate by presenting their privacy terms clearly and obviously to consumers (constituting proper notice of the terms) and subsequently giving consumers the choice to opt out of the data collection methods.[85] Notice and Choice are generally accepted as the appropriate standard for contracting with consumers online, but besides the economic pressure to appear on par with peer businesses, no mechanism can force compliance.[86]

D. Federal Law as an Unlikely and Ineffective Solution

Looking to the legislative history and the political climate, federal law seems to stand a minute chance of enactment. Additionally, with ambiguous Supreme Court guidance on the injury-in-fact requirement for standing under a federal law, it is uncertain what effect a private cause of action would have; the circuit courts still disagree on whether the future risk of harm after a data breach is sufficient to confer standing.

In 2016, the Obama-era Federal Communications Commission (FCC) enacted regulations that placed restrictions on how ISPs collect information on customers and how the companies notify customers of their collection and sharing practices.[87] The rules transferred enforcement power of ISPs to the FCC, a necessary move because the FTC was barred from regulating ISPs at that time.[88] In particular, the rules would have effectuated heightened disclosure requirements, an opt-in regime for the collection or use of personal information (for targeted advertising purposes), a broader definition of sensitive personal information, and a standard for data protection.[89] While only ISPs, like Comcast and Verizon, would have been regulated, the rules would have been a huge win for

---

[84] *Id*.
[85] Norton, *supra* note 22, at 195–96.
[86] The FTC has the ability to prosecute companies that, in following the Notice and Choice framework, post deceptive information to consumers, but cannot prosecute for failure to follow Notice and Choice. *Id*. at 195–97; *see* Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587, 599–600 (2007).
[87] *See generally* FCC, FCC 16-148, PROTECTING THE PRIVACY OF CUSTOMERS OF BROADBAND AND OTHER TELECOMMUNICATIONS SERVICES (2016); Devin Coldewey, *Everything You Need to Know About Congress' Decision to Expose Your Data to Internet Providers*, TECHCRUNCH (Mar. 29, 2017), https://techcrunch.com/2017/03/29/everything-you-need-to-know-about-congress-decision-to-expose-your-data-to-internet-providers [https://perma.cc/WBY9-TM3P].
[88] Coldewey, *supra* note 87.
[89] *Id*.

those in favor of privacy regulation and a step in the direction of greater transparency and consumer-centrism.

However, in March 2017, Congress overturned the rules, citing concerns with transferring power to the FCC and overburdening the ISPs with too much regulation.[90] President Trump approved Congress's action a few weeks later.[91] To make matters worse, the FCC is permanently prohibited from reintroducing a substantially similar bill.[92] It has been predicted that Trump's future policies will trend in the direction of deregulation or company-favored regulation.[93] Companies such as Facebook and Google have been lobbying the White House for a federal privacy law in the wake of California's 2018 privacy reform.[94] As idyllic of a solution as this seems, the motive behind the push is to create flexible federal law that preempts stricter state privacy standards, like those in California.[95] This type of preemptive federal law would overall weaken consumer protections by preventing individual states from enacting more stringent privacy laws.

Academics have presented many federal law solutions and broad privacy reform proposals. One proposed solution is a statute with data breach notification procedures that requires companies to reimburse reasonable mitigation expenses and gives consumers a private cause of action.[96] Another similarly would provide data breach notification procedures but enforce minimum data security standards through the FTC.[97] A third solution places similar requirements on companies but creates a private right of action with damages limited to mitigation expenses and attorneys fees.[98] Narrowing the scope to privacy policy regulation, one article proposes a privacy "nutrition label" that would

---

[90] S.J. Res. 34, 115th Cong. (2017) (enacted).
[91] Coldewey, *supra* note 87.
[92] *2017 ISP Privacy Regulations in the United States: All You Need to Know*, TECHRADAR (Apr. 10, 2017), http://www.techradar.com/news/2017-isp-privacy-regulations-in-the-united-states-all-you-need-to-know [https://perma.cc/L2YF-YREL].
[93] Cowan, *supra* note 19; Fung, *supra* note 19; *see also* Cecilia Kang, *Tech Industry Pursues a Federal Privacy Law, on Its Own Terms*, N.Y. TIMES (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html [https://perma.cc/V8YV-8VFY].
[94] Kang, *supra* note 93.
[95] *Id.*
[96] Patrick J. Lorio, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 127 (2017).
[97] Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45, 77 (2015).
[98] Cave, *supra* note 16, at 792.

increase notice to consumers based on the Nutrition Labeling and Education Act and enforced by the FTC.[99]

However, the overturned rules regulating ISPs are the ideal starting point for federal regulation with parallels to the disclosure regime, opt-in provisions, and requirements on data protection. The law would regulate privacy policies posted by anyone who collected PII about a consumer and should look something like this:

(1) Companies must post a privacy policy that is an enforceable agreement with consumers;
(2) companies must write their privacy policies in clear, plain language rather than dense legalese;
(3) companies must include specific and definite statements on their data safeguards and other privacy protections in place;
(4) consumers must have the ability to opt out of the company's data collection policies without having to stop use of the service; and
(5) individual victims of data breaches have a private right of action to sue companies for non-compliance with their policies.

A law with these features would provide the consumer with the ability to evaluate a company's security policies and decide whether or not to allow a company to use her information—eliminating the current binary choice of accepting the terms at face value or discontinuing use of the service.[100]

However, even with a federal statute that creates a private right of action for affected individuals, the law regarding Article III standing remains disputed. As will be discussed in the following section, given the continued circuit split, even if a federal data privacy law was enacted, courts could require a statutory violation to be accompanied by an underlying injury. Without the recognition of a risk of future harm as an injury-in-fact, consumers would still lack the ability to successfully litigate their claims.

[99] Corey A. Ciocchetti, *The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices*, 26 J. MARSHALL J. COMPUTER & INFO. L. 1, 40–41 (2008).

[100] Like federal law, a state law with the same characteristics may have a broad impact on all companies, like California's law requiring privacy policies. But even though enacting a state law may be a much more frictionless process than enacting a federal law, state law would only provide a private cause of action for that state's residents and would not accomplish the broader goal of providing a remedy for all consumers.

II. COMMON LAW DATA SECURITY CLAIMS

With a dearth of available remedial options under state and federal law, consumers frequently turn to common law claims to hold companies accountable after data breaches. As might be expected, these consumers are also met with infrequent success.

A. Article III Standing

Most plaintiffs in post-data breach suits do not even survive a preliminary review of their case.[101] Courts tend to stall consumer claims early on by refusing to confer Article III standing and dismissing the case, asserting that victims of a data breach have not suffered the requisite injury-in-fact. Because the standing requirement derives from the "case" or "controversy" language of Article III of the Constitution, the federal judiciary is confined by its limitations and may not hear a case where the plaintiff lacks standing.[102] Despite the state common law nature of the claims, class actions are prevalent in data breach situations; therefore, most cases are litigated in federal court.[103]

Prevailing on a state common law claim, such as negligence or breach of contract, most often requires an initial inquiry by the court to determine if the claim has met the threshold for Article III standing.[104] Article III first requires a plaintiff to show injury-in-fact before proceeding with her claim; injury-in-fact must be concrete and particularized and actual or imminent, not conjectural or hypothetical.[105] The plaintiff must then demonstrate that "the injury is fairly traceable to the challenged action of the defendant," and finally that "it is likely, as opposed to merely

---

[101] *See* Lorio, *supra* note 96, at 81; Megan Dowty, *Life Is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 686 (2017).

[102] Lujan v. Defs. of Wildlife, 504 U.S. 555, 559–60 (1992).

[103] J. Thomas Richie, *Data Breach Class Actions*, AM. BAR ASSOC., 44-SPG BRIEF 12, 14 (2015).

[104] U.S. CONST. art. III, § 2, cl. 1. While class actions present unique issues on class certification, such a discussion is outside the scope of this article, and it shall be assumed that victims in data breaches have suffered similar enough harm for approval of class certification. Richie, *supra* note 103, at 14–16. Even if cases are not litigated in federal court, most states have a similar standing requirement that must be met to proceed to a discussion of the merits of the case. Wyatt Sassman, *A Survey of Constitutional Standing in State Courts*, 8 KY. J. EQUINE AGRIC. & NAT. RESOURCES L. 349, 353–54 (2015–2016).

[105] Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000).

speculative, that the injury will be redressed by a favorable decision."[106] The Supreme Court's holding in *Clapper v. Amnesty International USA* clarified the imminence requirement: a threatened injury must be "certainly impending." [107] In other words, a plaintiff cannot just claim that she will be injured in the future without some evidence of certainty that the future injury will occur. While *Clapper* did not involve a data breach incident, it has become a standard in data breach litigation, cited both by courts justifying threatened injury as imminent and courts holding that threatened injury does not rise to the level of certainly impending.[108] In data breach cases, plaintiffs often are derailed by the injury-in-fact requirement, rather than the causation and redressability prongs. Therefore, this subsection will focus on the injury-in-fact analysis.

Often in a data breach case, plaintiffs find it difficult to prove harm that a court would recognize as injury-in-fact. Even when there has been actual identity theft, credit cards and banks will reimburse fraudulent charges, leaving no out-of-pocket damages. The increased threat of identity theft that follows a hacking incident is speculative, making it difficult to calculate any monetary loss. Given that the threat is merely speculative, courts may refuse to recognize mitigation expenses as imminently necessary. Currently, the circuit courts are split on whether threatened injury, such as the potential for identity theft post-data breach, constitutes injury-in-fact.[109]

The Second, Third, Fourth, and Eighth Circuits generally fall on one side of the split and find that an increased threat is pure speculation, requiring dismissal of the claim.[110] Alternatively, the Sixth, Seventh,

---

[106] *Id.*

[107] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013).

[108] Matthew George, *How Viable Is the Prospect of Enforcement of Privacy Rights in the Age of Big Data? An Overview of Trends and Developments in Consumer Privacy Class Actions*, 24 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 195, 197–200 (2015).

[109] Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, 92 NOTRE DAME L. REV. 1323, 1327 (2017).

[110] *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017) (denying standing because mere theft is insufficient: 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); *In re* SuperValu, 870 F.3d 763, 771 (8th Cir. 2017) (holding that without any allegations of actual misuse, future harm is not sufficient for standing); Reilly v. Ceridan Corp., 664 F.3d 38, 41 (3d Cir. 2011) (concluding 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); Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577, 580–83 (E.D.N.Y. 2015) (aff'd by 2d Cir., 689 F. App'x 89 May 2, 2017) (noting that without reason to think that the credit

Ninth, and D.C. Circuits have recognized the threat of future harm from a data breach as sufficiently definite and imminent to confer standing.[111]

The circuits against threat of future harm as injury-in-fact present an outdated view of data breach consequences: because actual misuse has not occurred, courts reason, there is no certainty that misuse will occur or that the hackers intended to commit identity theft with the victim's improperly accessed data. As such, the misuse of the information is just a speculative risk of some future occurrence and injury is not inevitable; therefore, mitigation efforts are unnecessary for many of the consumers involved. As the Fourth Circuit reasoned, standing may be found when there is a substantial risk of future harm, but even a thirty-three percent risk would mean that over sixty-six percent of customers suffered no harm.[112] Under this logic, the only way for a plaintiff to gain redress for a breach of her PII is to patiently wait for the resulting economic and non-economic (and thus non-compensable) consequences of a stolen identity. Further, the only way to receive compensation for purchasing credit monitoring services is if hackers kindly warned victims in certain terms that they would be stealing their identity in the future.

The circuits recognizing threat of future harm as injury-in-fact have made practical arguments: it is reasonable to assume that hackers will misuse the information they steal because the purpose of stealing information is to misuse it.[113] It is unreasonable to wait for actual misuse before incurring any mitigation expenses because the threat of misuse is substantial enough to be certainly impending.[114]

---

monitoring services plaintiff purchased were necessary and without evidence of loss of value in PII, increased risk of future harm was not certainly impending because it has been two years since the breach without fraudulent use of the data).

[111] *See, e.g.*, Attias v. Carefirst, Inc., 865 F.3d 620, 628–29 (D.C. Cir. 2017) (reasoning that "a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken"); Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) (stating 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"); Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 692–96 (7th Cir. 2015) (concluding that the injuries from resolving fraudulent charges and protecting against future identity theft were sufficient for injury-in-fact); Krottner v. Starbucks Corp., 628 F.3d 1139, 1141–43 (9th Cir. 2010) (holding that anxiety and stress, as well as time spent monitoring accounts was injury in fact even though no actual misuse of information was alleged).

[112] *Beck*, 848 F.3d at 276.

[113] *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016).

[114] *Id.* at 388–89.

It is becoming common advice for consumers affected by a data breach to enroll in credit monitoring services,[115] and many breached companies, like Equifax or Nationwide, offer a year or more of free enrollment.[116] The Sixth and Seventh Circuits have taken the offering of free credit monitoring as evidence that the company recognizes how substantial a threat the breach was.[117] However, the Fourth Circuit has rejected such reasoning because if providing credit monitoring services is seen as a concession that the threat was substantial, companies may refuse to offer such mitigating services to minimize their exposure in litigation.[118] In reality, these monitoring services often only provide minimal protection for a limited amount of time, and consumers must pay for a more upgraded service to receive the full protection recommended after a breach.[119] For example, purchasing credit monitoring services from Experian costs around $300 per year.[120] Consequently, regardless of

---

[115] *Identity Theft Protection Services*, FED. TRADE COMM'N, https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services [https://perma.cc/MH7H-J25V].

[116] One reason these companies likely do so is to minimize liability in litigation. If they provide credit monitoring services to consumers at no cost, then they avoid a judgment requiring them to pay for consumers' mitigation expenses. Unfortunately, these services only last for a certain period of time, often one year, and it is necessary to monitor credit for years after a data breach incident. Post-breach, Equifax offered a year of free credit monitoring services through a company it owned, but in agreeing to enroll in the services, consumers were required to submit their claims to arbitration. Ian C. Ballon, *Cybersecurity and Data Breach Litigation*, 3 E-COM. & INTERNET L. 27.07 (2017 update).

[117] Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 694 (7th Cir. 2015); *Galaria*, 663 F. App'x at 388.

[118] *Beck*, 848 F.3d at 276.

[119] *See* Jocelyn Baird, *We Signed Up for Equifax's TrustedID Premier and Here's What Happened*, NEXTADVISOR (Sept. 22, 2017), https://www.nextadvisor.com/blog/2017/09/22/we-signed-up-for-equifaxs-trustedid-premier-and-heres-what-happened [https://perma.cc/7G5X-EDSX]; Jeff Blyskal, *Expect Less and Pay More with Target's Credit Monitoring*, CONSUMER REPORTS (Feb. 6, 2014), https://www.consumerreports.org/cro/news/2014/02/expect-less-and-pay-more-with-target-credit-monitoring/index.htm [https://perma.cc/3WAK-WNTA]; Kelli B. Grant, *3 Reasons Breach Victims Might Not Want Equifax Credit Monitoring*, CNBC (Sept. 8, 2017), https://www.cnbc.com/2017/09/08/3-reasons-breach-victims-might-not-want-equifax-credit-monitoring.html [https://perma.cc/ZM2Y-PCNE].

[120] The Experian service is $24.99 per month with the first month priced at $4.99. For comparison, TransUnion credit monitoring is $19.95 per month and Lifelock credit monitoring ranges from $9.99 per month to $29.99 per month depending on coverage level. *Credit Monitoring*, EXPERIAN, https://www.experian.com/consumer-products/credit-monitoring.html [https://perma.cc/M2PE-WHSA]; *Credit Score Monitoring Services*, TRANSUNION, https://www.transunion.com/credit-monitoring [https://perma.cc/RY4W-U6UK]; LIFELOCK, https://www.lifelock.com/ [https://perma.cc/VT2X-LYJV].

whether a company provides mitigation services, consumers may have damages related to purchasing credit monitoring services. Taking a step back, courts should be promoting the use of mitigation tactics to reduce the potential destructive consequences of identity theft; preventative efforts will reduce overall harm to victims.

Overall, despite some circuits recently adopting a "future harm does not confer standing" stance, a large proportion of data breach cases are heard in California, where the courts are more favorable to recognizing that these preventative efforts confer standing. Furthermore, plaintiffs are having success by alleging forms of injury that do not rely on the recognition of future harm.[121] The Eighth Circuit, while refusing to confer standing for claims of future harm in *In re SuperValu*,[122] has taken a more consumer-friendly view when looking at injury in breach of contract cases. Arguing that they have lost a "benefit of the bargain," plaintiffs have been granted Article III standing for injuries from overpaying for security measures they contracted for but never received.[123]

It appears that as the amount of data breach litigation increases, courts are beginning to understand the realities of the impacts of data breaches on consumers and are moving towards more victim-friendly results; decisions are trending toward recognizing future harm as injury-in-fact for Article III standing purposes.[124] This trend could have a larger impact than just increasing judicial remedies for consumers. It could pave the way for broader federal reform.

An anticipated 2016 Supreme Court decision, *Spokeo, Inc. v. Robins*, expected to clear the air about standing under federal law in data breach cases, only created more confusion.[125] The case involved Spokeo, a

---

[121] This success is limited. While the Eighth Circuit has granted standing for overpayment in breach of contract claims, these claims were subsequently dismissed for failure to state a claim. *See* Carlsen v. GameStop, Inc., 833 F.3d 903, 910–12 (8th Cir. 2016); Kuhns v. Scottrade, Inc., 868 F.3d 711, 716–18 (8th Cir. 2017). *But see In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783, at *12–16 (N.D. Cal. May 27, 2016) (denying a motion to dismiss for failure to state a claim, asserting that a breach of contract claim with damages of overpayment, loss of value of PII, and mitigation expenses was sufficiently alleged).

[122] *In re* SuperValu, Inc., Customer Data Security Breach Litigation, 870 F.3d 763, 771–73 (8th Cir. 2017).

[123] *See, e.g.*, *Kuhns*, 868 F.3d at 716; *Carlsen*, 833 F.3d at 909–10; *In re* VTech Data Breach Litig., No. 15 CV 10889, 2017 WL 2880102, at *5 (N.D. Ill. July 5, 2017).

[124] Allison Grande, *Data Breach Suits Find Easier Path With D.C. Circ. Ruling*, LAW360 (Aug. 3, 2017, 10:47PM), https://www.law360.com/insurance/articles/951179/data-breach-suits-find-easier-path-with-dc-circ-ruling [https://perma.cc/49PD-MYXQ].

[125] John Seiver & Bryan Thompson, *Supreme Court's "Standing" Ruling in Spokeo and Its Impact on Pending and Future Litigation*, DAVIS WRIGHT TREMAINE LLP (June 9, 2016), http://www.dwt.com/Supreme-Courts-Standing-Ruling-in-Spokeo-and-Its-Impact-on-Pending-and-Future-Litigation-06-09-2016/ [https://perma.cc/AB33-WZ3V].

"people search engine" that published incorrect information about a consumer who claimed he was unable to find employment because of the misrepresentation.[126] The consumer sued under the Fair Credit Reporting Act (FCRA) in a case that the district court dismissed, stating that he alleged only a procedural violation of the law and thus lacked injury-in-fact.[127] The Ninth Circuit reversed, and the Supreme Court took on the controversy to decide whether a violation of a federal statute in itself is sufficient injury for standing or whether the violation must cause harm that independently survives an injury-in-fact analysis.[128]

The Court held that the plaintiff "cannot satisfy the demands of Article III by alleging a bare procedural violation" because a violation of one of the FCRA procedural requirements may lead to no harm.[129] Post-*Spokeo*, courts have used the decision to further their prior stances on future threat of harm as appropriate for standing.[130] Those that have limited injury-in-fact to actual harm, rather than future harm, have interpreted the opinion narrowly to require underlying damage in order for a statutory violation to confer standing.[131] Those circuits more welcoming to future threat of harm arguments have interpreted the decision more broadly.[132] As alluded to earlier, without a resolution of the circuit split on standing, federal law could remain minimally effective. But if courts were to consistently recognize the threat of future harm as injury-in-fact, plaintiffs would be able to successfully proceed with both their common law claims and claims under future federal regulation.

B. Theories of Liability

Even when plaintiffs overcome the standing obstacle, their chances of recovery remain bleak. Courts have been even more reluctant to resolve claims in plaintiffs' favors, often because plaintiffs have struggled to prove negligent behavior, the existence of some contractual obligation, or some other legally improper conduct by the defendant. And despite recognizing injury, courts can have difficulty calculating damages or finding an appropriate remedy. Moreover, most data breach cases settle

---

[126] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1544 (2016).
[127] *Id.*
[128] *Id.* at 1545.
[129] *Id.* at 1550.
[130] Hanley Chew & Eric Ball, *Ninth Circuit in Spokeo: Inaccurate Consumer Reports Support Standing in FCRA Cases*, FENWICK & WEST, LLP (Aug. 17, 2017), https://www.fenwick.com/publications/pages/ninth-circuit-in-spokeo-inaccurate-consumer-reports-support-standing-in-fcra-cases.aspx [https://perma.cc/4RTQ-BD38].
[131] *Id.*
[132] *Id.*

prior to litigation, eliminating the chance of creating precedent to aid future parties with similar claims.

Plaintiffs have employed numerous strategies to hold companies liable for failing to maintain personal information appropriately. These theories have included negligence, misrepresentation, invasion of privacy, unjust enrichment, and breach of contract, among others. Rarely has a claim under one of these theories enabled a plaintiff-victim to succeed in obtaining relief. As a result, most common law claims settle. However, as this article will discuss in Part III, a breach of contract claim appears to have the most potential to cater to courts' demands.

One prevalent claim that data breach defendants face is negligence for failure to adopt proper security measures. However, even plaintiffs that convince the court that the defendant breached a duty to consumers by failing to use reasonable security measures often have difficulty proving more than purely economic damages.[133] Thus, the economic loss doctrine precludes most negligence claims.[134] Even if a plaintiff could withstand Article III inquiry, an often ill-equipped court would then be tasked with using its discretion in determining reasonableness of security protocols.

Plaintiffs have tried to hold companies accountable to their privacy policies by alleging misrepresentation of data protection efforts.[135] But a misrepresentation claim requires a showing of reliance on the misleading information.[136] In order to prove reliance, a consumer must prove that they actually read the policy, a standard with a high bar to overcome.[137] Clicking a button acknowledging that you have read the policy does not pass the "actually read" standard, nor does physically clicking or scrolling through the text of the policy show that you actually read the material.[138]

Invasion of privacy claims have been similarly fruitless. In some states, clearing the high bar for an invasion of privacy claim requires a showing that the act is considered highly offensive to a reasonable

---

[133] *See, e.g.*, *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 967, 973 (S.D. Cal. 2014), *order corrected*, No. 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014) (recognizing that Sony breached a legal duty to the Plaintiffs by failing to employ reasonable security measures, but dismissing the negligence claim because Plaintiffs suffered purely economic losses).

[134] Peter J. Arant, *Understanding Data Breach Liability: The Basics Every Attorney Should Know*, 40 MONT. LAW., Feb. 2015, at 11; *see*, *e.g.*, *In re* Zappos.com, Inc., No. 3:12-CV-00325-RCJ, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013), *petition for cert. filed*, (U.S. Aug. 20, 2018) (No. 18-225); *In re Sony Gaming Networks*, 996 F. Supp. 2d at 967, 973.

[135] *In re* Yahoo! Customer Data Security Breach Litigation, No. 16-MD-02752-LHK, 2017 WL 3727318, at *25 (N.D. Cal. Aug. 30, 2017).

[136] *Id*.

[137] *Id*. at *27.

[138] *Id*. at *27–28.

person.[139] For example, California courts have deemed theft of Social Security numbers—personal data often regarded as the most sensitive—insufficiently offensive to qualify as invasion of privacy.[140] Other states require the information to be distributed to the public at large.[141]

Unjust enrichment claims are only available to consumers who paid for the services of a business, limiting their applicability in data breaches.[142] Standards differ from state to state, with California even refusing to recognize unjust enrichment as an independent cause of action.[143] Consumers have found it extremely difficult to prove that part of the service price was intended for data security and that by failing to protect consumer data, the company was unjustly enriched when users received less value than they bargained for.[144]

Consumers have also attempted claims of emotional distress, yet in courts with more flexible interpretations of injury and in courts with less consumer-friendly histories in data breach cases, these claims have been unsuccessful.[145]

Despite common law hurdles, breach of contract theories could be a viable litigation avenue to enforce statements made in corporate privacy policies. Because privacy policies presented in clickwrap form are validly agreed to by plaintiffs and companies alike, the descriptions of companies' data security measures within the policies are often sufficiently definite, and because courts are trending towards recognizing certain forms of consumer loss as damages, victims may be able to finally move towards successful trial outcomes under common law breach of contract theories. The following section presents a solution where consumers can focus their efforts on breach of contract claims as a method of redress.

---

[139] Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1024–25 (N.D. Cal. 2012).

[140] *See id.*; *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012).

[141] *See* Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d. 646, 662 (S.D. Ohio 2014); Burton v. MAPCO Exp., Inc., 47 F. Supp. 3d 1279, 1287–88 (N.D. Ala. 2014).

[142] Douglas H. Meal & David T. Cohen, ROPES & GRAY LLP, *Private Data Security Breach Litigation in the United States*, 2014 WL 10442, at *7 (Jan. 2014).

[143] *Id*.

[144] *See, e.g.*, Carlsen v. GameStop, Inc., 833 F.3d 903, 912 (8th Cir. 2016).

[145] *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 45 (3d Cir. 2011) (rejecting emotional distress claims because "[t]he hacker did not change or injure Appellants' bodies; any harm that may occur—if all of Appellants' stated fears are actually realized—may be redressed in due time through money damages after the harm occurs with no fear that litigants will be dead or disabled from the onset of the injury"); Barnes & Noble Pin Pad Litig., No. 12-CV-8617, 2013 WL 4759588, at *5 (N.D. Ill. Sept. 3, 2013) ("Emotional distress in the wake of a security breach is insufficient to establish standing, particularly in a case that does not involve an imminent threat to the information."); *In re* VTech Data Breach Litig., No. 15 CV 10889, 2017 WL 2880102, at *5 (N.D. Ill. July 5, 2017) ("Where only an unspecified risk of future financial harm is alleged, emotional distress in the wake of a data security breach is insufficient to establish standing.").

III. BREACH OF CONTRACT CLAIMS AS A SOLUTION

This section will present a feasible, albeit limited, solution for the lack of consumer data protection. The solution presents a temporary way to take advantage of a trend occurring in certain circuits, giving consumers a viable chance to recover damages from companies with lax security standards when their data is improperly accessed. Even though the ideal solution, and the cleanest, is the aforementioned federal regulation of data security and privacy policies, the country is not ready to take that leap. The ideas this section will present could help set the stage for broad privacy reform and move litigation away from the current dynamic where big business has a disproportionate amount of power when consumers seek redress for the damages they suffer post-data breach.

This paper proposes the following multi-part recommendation: 1) courts should move to recognize threat of future harm as injury-in-fact that is concrete and particularized and actual or imminent, not conjectural or hypothetical; 2) courts should treat privacy policies as enforceable agreements, binding companies to their statements on data protection; and 3) courts should recognize mitigation expenses, along with other theories of economic injury, as consequential and direct damages caused by the company's breach of its privacy policy. The realization of these three prongs would allow a consumer breach of contract claim to prevail, giving data breach victims much deserved compensation.

A. Article III Standing

As discussed in Part II, courts should begin to consistently recognize a threat of future harm as sufficient to confer standing in data breach cases. The remaining circuits (including those that have classified future harm as too speculative to constitute injury-in-fact) should follow the lead of the Sixth, Seventh, Ninth, and D.C. Circuits and allow victims to proceed to a hearing on the merits of their claims. Even if courts refuse to do so, they can confer standing for breach of contract damages such as overpayment or loss of PII value without having to recognize any threat of harm as imminent. The ultimate goals of this solution are to 1) provide temporary relief through the judicial system to consumers who have suffered misuse of their data and 2) subsequently set the stage for comprehensive federal reform. Improving outcomes for plaintiffs struggling to meet standing requirements would move the courts to a judicial remedy for data breaches, but in light of *Spokeo's* ambiguity, it would also give maximum effectiveness to a federal law with a private right of action.

B. Presentation and Language of Privacy Policies

Despite the lack of federal law requiring privacy policies, there are a few reasons why companies choose to post them. As mentioned above, state laws like CalOPPA incentivize companies that may reach California residents to comply with California laws. The FTC's industry-standard Notice and Choice guidelines prescribe disclosure of privacy practices to users. Other countries, like those in the European Union,[146] may mandate disclosures to users. U.S.-based businesses who expect to transact with international consumers or have operations overseas may choose to meet those standards as well.

1. Privacy Policies as Clickwrap Agreements

Typically, privacy policies are presented along with a company's terms of use when creating an online account. Most commonly, when websites offer the user the ability to create an account, the user must agree to both the terms of use and the privacy policy in order to access the service. For a representative example, on Twitter, a prospective accountholder will enter her name and email and choose a password before proceeding to click the "Sign Up" button.[147] Directly beneath the "Sign Up" button is the message: "[b]y signing up, you agree to the Terms of Service and Privacy Policy."[148] The words "Terms of Service" and "Privacy Policy" are in blue font, signaling a hyperlink to pages displaying the full text of the two documents.[149] The presentation of the language of assent constitutes adequate notice to the consumer (this presentation style indicates a "hybridwrap" or "sign-in wrap" agreement[150]).[151] The

---

[146] *EU Privacy Policy*, TERMSFEED (Oct. 20, 2017), https://termsfeed.com/blog/eu-privacy-policy [https://perma.cc/JP62-F8QE].
[147] TWITTER, https://twitter.com/signup [https://perma.cc/ZME7-2L25].
[148] *Id.*
[149] *Id.*
[150] The term hybridwrap originated because these agreements have characteristics of both browsewrap and clickwrap agreements. Browsewrap agreements are generally unenforceable because they do not give proper notice to the user nor do they require affirmative assent. In cases of browsewrap, links to the terms of use and privacy policies are placed inconspicuously on the website, often requiring the user to scroll to the bottom of the page or search through links on the website to find the text. Hybridwrap agreements do not go so far as to require the level of affirmative assent that clickwrap agreements do but they give the user adequate notice, making the agreements in general enforceable. *See* Fteja v. Facebook, Inc., 841 F. Supp. 2d 829, 834–40 (S.D.N.Y. 2012) (recognizing presentation of terms in a form with elements of both browsewrap and clickwrap, though not explicitly creating a term for it); *see also* Berkson v. Gogo, LLC, 97 F. Supp. 3d 359, 394–401 (E.D.N.Y. 2015).

consumer now has the ability to review both documents before agreeing to them and always has the option to discontinue the account creation process if she disagrees with any of the terms.[152] Most companies have a similar account creation process, though some choose to increase the level of notice given to the consumer. They do so by forcing active assent in the form of a mandatory checkbox (known as a "clickwrap agreement") or requiring the consumer to open the documents and physically scroll through the text before they are given the option to proceed with registration ("scrollwrap agreements").[153] The higher the level of notice a consumer is given, the more likely the contract is an enforceable agreement.[154]

Terms of use agreements, when validly presented to the consumer in hybridwrap, clickwrap, or scrollwrap form, such as in the above example, are enforceable contracts[155] and are intended to be enforceable so that companies can bind aggrieved consumers to arbitration agreements and limits on damages. However, privacy policies are written with the intention of being an unenforceable statement of policy, so consumers cannot hold companies accountable for any inaccuracies or breaches. The result is a pair of documents presented to the consumer at the same time and in the same manner, yet one is an enforceable contract and one is completely unenforceable. Consumers get the short end of the stick; companies make sure account-holders are legally bound by complex, unilaterally-drafted agreements but refuse to bind themselves to their statements on data security and other privacy issues. Oftentimes companies use terms of use agreements against a plaintiff suing for breach to force the consumer to arbitrate rather than litigate.[156] In other cases where the user has agreed to limit the company's liability for damages, the company will seek to enforce that limit to prevent any payouts to consumers.[157]

---

[151] The presentation of the agreement matters greatly. It is important that "Terms of Service" and "Privacy Policy" are clearly distinguished from the rest of the sentence through noticeable color difference. Similarly, the language of agreement must be presented in close proximity to the "Sign Up" button. Nguyen v. Barnes & Noble, 763 F.3d 1171, 1177–78 (9th Cir. 2014).

[152] TWITTER, *supra* note 147.

[153] Berkson, 97 F. Supp. 3d at 394–401.

[154] *See* Erin Canino, *The Electronic "Sign-in-Wrap" Contract: Issues of Notice and Assent, the Average Internet User Standard, and Unconscionability*, 50 U.C. DAVIS L. REV. 535, 540–41 (2016).

[155] Berkson, 97 F. Supp. 3d at 394–401.

[156] *See*, *e.g.*, Tompkins v. 23andMe, Inc., No. 5:13-CV-05682-LHK, 2014 WL 2903752 (N.D. Cal. June 25, 2014), *aff'd*, 840 F.3d 1016 (9th Cir. 2016).

[157] *See In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, at *46 (N.D. Cal. Aug. 30, 2017).

2. Sufficiently Definite Language

The disparity in enforceability stems from the language of the policy. Companies, advised by their attorneys, use vague and ambiguous language to describe their privacy practices, making sure to create terms indefinite enough to preclude any breach of contract claims. Courts have reaffirmed this practice by classifying certain language in a privacy policy as non-actionable puffery.[158]

Nevertheless, this section argues that most websites' privacy policies actually do contain language that is definite enough to constitute a promise that a consumer can rely on. Many privacy policies state not only that they employ safeguards to protect information, but use language along the lines of "we take reasonable measures to protect your information." Reasonable standards are always changing as technology advances, but the FTC has taken examples from past enforcement actions to compile some reasonable security measures: using encryption (either Transport Layer Security or Secure Sockets Layer) or cryptographic hash, segmenting the network with firewalls, and some more common sense tactics like minimizing unnecessary data collection, restricting employee access to data, and requiring secure passwords.[159]

Looking at the top visited websites in the United States,[160] fifty-five out of seventy-one of the companies' privacy policies list some sort of standard of security measure that they maintain (for example, reasonable, industry standard, adequate, or strong security measures) or some type of specific security measure they take (such as encryption, using Secure Sockets Layer software, or Transport Layer Security).[161]

If state standard of care statutes can require maintenance of undefined "reasonable standards" of protection, then companies that use that same language in their privacy policies should be held accountable for those statements.[162] Additionally, the Northern District of California in *In*

---

[158] *Id*. at *25 (determining that the statement "protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users' trust" is nonactionable puffery because it does not specifically characterize the defendant's services).

[159] *See generally* FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [https://perma.cc/S8GC-5BQW].

[160] The top visited websites were collected based on Alexa rankings of websites with the highest traffic at various points in 2017 and 2018. *Top Sites in United States*, ALEXA, https://www.alexa.com/topsites/countries/US [https://perma.cc/6962-KPRC].

[161] This data was collected by the author. The full results and analysis are on file with the author.

[162] California's standard of care statute states: "A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain

re Yahoo! Customer Data Breach Litigation classified statements in Yahoo!'s privacy policy that the company offers "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you" as a "specific, non-subjective guarantee."[163] Statements similar to this could be considered actionable in a breach of contract claim, especially since the court noted that the statement was definite enough for consumers to reasonably rely on.[164] Even though Yahoo! only promised to comply with federal regulation (which is minimally protective at best), the court interpreted its statement to mean that its safeguards "were sufficient to protect users' information from ordinary data security threats."[165]

Therefore, if consumer agreement to the contract is in clickwrap form, an enforceable mechanism of contracting, and the provisions concerning data security methods are sufficiently definite to constitute a promise, then plaintiffs should have a valid breach of contract claim against companies that suffer data breaches due to lax data protection policies.

Some companies, like Facebook and Reddit, appear to have taken advantage of a risk-eliminating loophole that ensures their privacy policy is never construed as an enforceable agreement.[166] These companies have made one small but significant change in the text of their assent language: "[b]y clicking Create Account, you agree to our Terms and that you have read our [Privacy] Policy."[167] Instead of agreeing to both the terms of use and privacy policy, the user is agreeing to abide by the terms of use but is only agreeing that she has *read* the privacy policy. This loophole is one limitation of the breach of contract theory.[168] If more companies begin to follow Facebook and Reddit's lead, consumers technically will not have

---

reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." CAL. CIV. CODE § 1798.81.5(b); *see also* 201 MASS. CODE. REGS. 17.01–05.

[163] No. 16-MD-02752-LHK, 2017 WL 3727318, at *26 (N.D. Cal. Aug. 30, 2017). In this case, the plaintiffs alleged two statements in Yahoo!'s privacy policy were misleading. The first (referenced in note 135) was considered puffery by the court. The second, discussed here, was not puffery. Even though the statements were made in the context of a misrepresentation claim, they have broad applicability to the breach of contract context.

[164] *Id*.

[165] *Id*.

[166] *See* FACEBOOK, facebook.com [https://perma.cc/ZM5Z-W7CS]; REDDIT, reddit.com [https://perma.cc/9C2W-H6RH].

[167] FACEBOOK, *supra* note 166; REDDIT, *supra* note 166.

[168] Another loophole would be removing any language on data security or what types of security measures the company takes. However, doing so could cause negative customer reactions and undesirable publicity.

agreed to abide by the privacy policy and thus may not be able to claim injury.[169] Currently though, almost all of the top visited websites in the United States still present their assent language in the traditional manner.[170]

C. Theories of Recovery

Plaintiffs may have a valid argument that a company's privacy policy is an enforceable clickwrap agreement, but without damages, any breach of contract claims will be dismissed. Plaintiffs in breach of contract suits face the same hurdles as plaintiffs in any other data breach lawsuit when it comes to damages: courts have been reluctant to assign value to PII and recognize injury-in-fact.

The theory most likely to prevail is payment of mitigation expenses to prevent identity theft after a data breach. The main reason why courts have been reluctant to accept the cost of credit monitoring services and other mitigation expenses is because they remain skeptical about the necessity of the purchase. *Clapper* stated that plaintiffs "cannot manufacture standing by incurring costs in anticipation of non-imminent harm," so courts must first accept the threat as imminent before considering mitigation damages.[171] Courts have argued that because future identity theft is speculation, mitigation expenses are non-essential and overly cautious. However, as knowledge of the far-reaching implications of data breaches propagates and stories of breach after breach pervade the news cycle, judges must shift their reasoning to be more up-to-date on the realities of the information age. Some courts have already taken this stance, granting Article III standing to plaintiffs alleging payment of mitigation expenses as injury-in-fact.[172] Such a stance assumes that future threat of injury is imminent, justifying the need to purchase credit monitoring services or the like.

Another theory of damages that some courts have begun to recognize is overpayment for services.[173] If a company guarantees certain data storage practices in its contractual arrangements with customers, theoretically some portion of the price paid for the service goes toward

---

[169] It is unclear how courts will treat this change in assent language. It may not preclude a promissory estoppel claim where a consumer relies on the language of the privacy policy.
[170] *See supra* note 161.
[171] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1155 (2013).
[172] Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388–89 (6th Cir. 2016); Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 694 (7th Cir. 2015).
[173] Kuhns v. Scottrade, 868 F.3d 711, 716 (8th Cir. 2017); *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783, at *14 (N.D. Cal. May 27, 2016).

compliance with those statements. Thus, when a company has provided inadequate data security, the consumer is damaged in the "amount equal to the difference between the value of the subscription that he paid for and the value of the subscription that he received, i.e., a subscription with compromised privacy protection."[174] Of course, this argument only has effect when accountholders have paid for access to a service, a limited percentage of cases. Most websites that consumers register for, like social media, retail shopping, or email services, offer free accounts.

An alternative argument that plaintiffs have attempted is that their PII has economic value that is diminished when the company failed to protect it. The Ninth Circuit has recognized diminution in value of PII as valid damages for a breach of contract claim.[175] This theory often presents itself as a loss of sales value of PII. Using the logic that PII has sales value and when hackers access it for free and reap profits from the sale, opportunities for plaintiffs to sell their PII have been foreclosed.[176] The Northern District of California in *In re Anthem, Inc. Data Breach Litigation* stated that plaintiffs can show diminution in value of PII with evidence of either existence of an economic market for the information or that it would be more difficult to sell the information post-breach.[177]

These three theories of damages incurred by breach of contract would help to give consumers remedies for their stolen information. Despite a minority of courts recognizing these theories, their success is not unprecedented. Even for courts that remain skeptical about the risk of future harm as impending injury, overpayment and diminution of value of PII do not require any extrapolation of risk.

---

[174] Carlsen v. Game Stop, 833 F.3d 903, 909 (8th Cir. 2016); *see also In re* VTech Data Breach Litigation, No. 15 CV 10889, 2017 WL 2880102, at *5, (N.D. Ill. July 5, 2017).

[175] Svenson v. Google Inc., No. 13-CV-04080-BLF, 2016 WL 8943301, at *9 (N.D. Cal. Dec. 21, 2016).

[176] *See In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, at *14 (N.D. Cal. Aug. 30, 2017) ("Plaintiffs' allegations that their PII is a valuable commodity, that a market exists for Plaintiffs' PII, that Plaintiffs' PII is being sold by hackers on the dark web, and that Plaintiffs have lost the value of their PII as a result, are sufficient to plausibly allege injury.").

[177] *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016) ("'With access to an individual's [PII], criminals can do more than just empty a victim's bank account—they can also commit various types of fraud . . . [they] may obtain a job using the victim's Social Security Number.' These allegations could be read to infer that an economic market existed for Plaintiffs' PII, and that the value of Plaintiffs' PII decreased as a result of the Anthem data breach") (internal citation omitted.).

D. Scope

It is worth noting that this solution is extremely limited in scope but could prove effective in moving the legislature in the direction of comprehensive federal privacy reform. Here are some of the limitations and assumptions:

(1) This solution is largely focused on US-based companies that store data on US consumers.
(2) The companies involved in data breach litigation must present their users with a privacy policy upon creation of an account with the company, regardless of whether the user pays for the service or accesses it for free.
(3) The users must validly agree (in clickwrap or other enforceable form) to the company's privacy policy, not just that they have read the privacy policy.
(4) Within the privacy policy, the company must state some sort of minimum data security standard.
(5) As mentioned above, given that most consumer privacy actions are class action suits, this solution assumes that the claims presented by consumers, while they are state breach of contract claims, are class action lawsuits in federal court.
(6) Finally, this solution only covers the presentation of data security standards by companies in their privacy policies and does not cover statements on collection or use of data by such companies, despite the privacy implications of those statements.

E. Breach of Contract Claims as the Initial Step in a Broader Objective

The plan this paper proposes brings data breach litigation to a place where *Spokeo's* unclear meaning is rendered irrelevant. If future risk of harm after a data breach were always found to be sufficiently imminent for an injury-in-fact determination, violations of a federal data breach statute would constitute standing. The court would not be required to do any analysis on whether the violation is merely procedural because all violations will constitute harm with damages independently sufficient for Article III standing. At that point, the stage would be set for federal legislation (assuming Congress's approval) to become an effective enforcement mechanism.

In an ideal world, federal regulation should be based on freedom of contract principles; companies will present their data protection standards in definite, binding terms to consumers, and consumers will make an educated choice whether or not to give the companies use of their personal information. Federal law should not give requirements for data protection

measures; the standard should be decided by the market. Any standards for data protection codified in statute must be based on vague-enough standards to allow for technological advances or risk specific standards becoming obsolete. Either approach is suboptimal. But, give the consumer who disagrees with a company's data protection standards the choice to opt-out of use of her PII, and companies will have to be responsive to consumer preferences.

IV. CONCLUSION

Despite the soundness of the proposed solution, this article leaves many questions unanswered and many topics undiscussed. If courts start to more consistently grant standing and rule for the plaintiffs, there may be an influx of lawsuits filed. Courts may not have the resources to properly handle a substantial increase in litigation. And if companies are required to reimburse victims for losses after being held accountable to statements made in their privacy policies, they might begin to remove any definite language to which they could be held liable. Alternatively, companies may add or enforce existing security standards in their privacy policies with which consumers must abide, for example, not sharing their password or using the same password on multiple websites. Consumers who breach their security duties may be held liable by those companies for contributing to the risk of breach. By no means does this judicial solution solve every problem related to data security lawsuits; this is why the ultimate objective should be comprehensive federal privacy reform.

In a world where it is virtually impossible to function in society without email and social media accounts, blind acceptance of companies' privacy terms is effectively mandatory. More data breach incidents are occurring than ever before, and consumers are swindled at both ends. When initially registering for a service, consumers are forced to agree to one-sided, company-favorable terms in a debatably unconscionable bargaining situation. Then, when companies fail to adequately protect consumer data, data breach victims have little recourse against those companies. This needs to change—first in the judiciary and ultimately by Congress' hand.

APPENDIX A

Federal Data Privacy Statutes

Federal Law	**Who does it regulate?**	**What does the law require?**	**Enforcement**
Health Insurance Portability and Accountability Act (HIPAA)[1]	Entities that store protected health information. (Generally, all clinics, medical providers, hospitals, pharmacies, health insurance companies and government-sponsored health care programs)	Requires "appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization"	Affected individuals can submit complaints, but enforcement is carried out by the Department of Health and Human Services Office for Civil Rights Private right of action: No
Fair Credit Reporting Act (FCRA)[2]	Credit reporting agencies that assemble and sell credit and financial information about consumers	Requires implementation of safeguards by using reasonable procedures to detect, prevent, and mitigate identity theft of any accounts the agencies maintain	Private right of action: Yes

[1] Health Insurance Portability and Accountability Act of 1996 (HIPAA) Pub. L. No. 104-191, 110 Stat. 1936; *Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html [https://perma.cc/9FJS-3C6X]; *The HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/index.html [https://perma.cc/E6QX-F33U]; *Enforcement Process*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html [https://perma.cc/3PEH-WP4D].

[2] 15 U.S.C. § 1681c-1 (2018); *The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report*, ELEC. PRIVACY INFO. CTR, https://epic.org/privacy/fcra/#introduction [https://perma.cc/3XA2-DGZ9].

Gramm-Leach-Bliley Act (GLBA)[3]	Financial institutions that offer financial products and services (such as loans, investment advice or insurance) to consumers	Requires financial institutions to give consumers privacy notices as to what nonpublic personal information is collected, and when and to whom data is disclosed; the company must take measures to secure the consumer information and provide an accurate description of those security measures in its privacy notice	Enforcement is carried out by the FTC Private right of action: No
Family Educational Rights and Privacy Act (FERPA)[4]	Schools and other educational institutions that maintain student educational records (of both minor and adult students)	Institutions must maintain certain privacy protections over the records they store	Students alleging violations can submit complaints to the Family Policy Compliance Office in the U.S. Department of Education Private right of action: No

[3] Gramm-Leach-Bliley Act (GLBA) P.L. 106-102, 113 Stat. 1338 (1999); *Gramm-Leach-Bliley Act*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act [https://perma.cc/UG5L-QG94]; *How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, FED. TRADE COMM'N (July 2002), https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm#disclosure [https://perma.cc/2WAV-GS89].

[4] 20 U.S.C. § 1232(g); *Family Educational Rights and Privacy Act (FERPA)*, U.S. DEP'T OF EDUC., https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html [https://perma.cc/U95K-RYSA].

Children's Online Privacy Protection Act (COPPA)[5]	Any business that directs service at or collects the information of a child under the age of 13	Website operators "must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children" and must only release a child's information to third parties who provide comparable assurances	Enforced under the FTC's authority to prosecute unfair or deceptive trade practices Private right of action: No

[5] 16 CFR § 312.8; *Children's Online Privacy Protection Rule ("COPPA")*, FED. TRADE COMM'N (Apr. 2002), https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule [https://perma.cc/ARL6-Q96Q].