Journal of Technology Law & Policy

Volume 24 | Issue 1 Article 3

The Data Breach Epidemic: A Modern Legal Analysis

Laura A. Hendee

THE DATA BREACH EPIDEMIC: A MODERN LEGAL ANALYSIS

Laura A. Hendee[*]

Abstract

This Note sheds light on the major legal issues surrounding the numerous data breaches that plague our modern technology-driven society. Current laws in the United States vary widely in how they handle the resolution of harm to unsuspecting victims of data breaches. The issue of Article III standing is commonly at the forefront of the conflict and discussion in this area, which has resulted in a substantial circuit split in the United States. The newly enacted California Consumer Privacy Act will likely have a major impact in this area of the law and will undoubtedly influence how consumers' personal information is handled in the years to come.

* LL.M. Taxation Candidate, New York University School of Law (2021); J.D., University of Florida Levin College of Law (2020); M.S.T., University of Miami (2016); B.S.B.A. Accounting, University of Miami (2016).

INTRODUCTION

It seems like every day there is a new article headline in the news or new email in your inbox stating something to the effect of, "Company X Announces New Data Breach," or the even more alarming, "We found your information in another company's data breach." In reality, it does not just seem like it: on average, there *are* new company data breaches every day.[1] In fact, Privacy Rights Clearinghouse reports that there have been over 9,600 data breaches since 2005, exposing over 11,500,000,000 personal records.[2] These are disturbing statistics, and as the variety of industries and types of businesses impacted by breaches each year continue to increase, many consumers are beginning to realize that such breaches have become "the new normal."[3] The question is not "if" a breach will occur, but "when" a breach will occur.[4]

A "data breach" is defined as "a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion."[5] They can be caused by many things, including but not limited to weak passwords, missing software patches that are exploited, lost or stolen electronic devices, unauthorized exposure during information transit, hackers exploiting unsecured wireless networks, and social engineering (i.e., email phishing).[6] With so many data breaches occurring each year, several of them large in terms of the number of impacted individuals and the volume of data acquired, it follows that a number of those individuals are taking action.[7] Such data breaches frequently make headlines and provoke litigation brought by

---

1. *See* Davey Winder, *Data Breaches Expose 4.1 Billion Records in First Six Months of 2019*, FORBES (Aug. 20, 2019, 6:31 AM), https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/. *See also* Daniel Funke, *By the Numbers: How Common Are Data Breaches—and What Can You Do About Them?*, POLITIFACT (Sept. 23, 2019), https://www.politifact.com/article/2019/sep/23/numbers-how-common-are-data-breaches-and-what-can-/.

2. *See* Daniel Funke, *supra* note 1.

3. *See* IDENTITY THEFT RES. CTR., 2018 END-OF-YEAR DATA BREACH REPORT (Jan. 28, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

4. *Id.*

5. Margaret Rouse, *Essential Guide: GDPR Compliance Requirements for CRM Managers—Definition: Data Breach*, SEARCHSECURITY, (last updated May 2019) https://searchsecurity.techtarget.com/definition/data-breach.

6. *Id.*

7. *See* David Balser et al., *Insight: Data Breach Litigation Trends to Watch*, BLOOMBERG L. (Mar. 4, 2019, 4:01 AM), https://news.bloomberglaw.com/privacy-and-data-security/insight-data-breach-litigation-trends-to-watch.

consumers, often leading to large class action lawsuits.[8] After the passage of the Class Action Fairness Act,[9] most data breach lawsuits have been brought in federal court.[10] Because of the lack of clarity provided by courts and legislatures in the area of data privacy litigation, some of the most noteworthy data breach litigation developments in 2018 resulted in large consumer class action settlements.[11] This settlement trend will likely continue unless further guidance is provided or a more clearly defined legal standard develops surrounding the implementation of reasonable security measures that are effective in the current state of advancing technology and cybersecurity.[12]

One of the major reasons for the lack of clarity regarding data breach litigation outcomes across the country spurs from the circuit split on the issue of standing.[13] Courts dismiss many of these data breach cases because plaintiffs lack a cognizable injury-in-fact, which is a major component for Article III standing.[14] Generally, the First, Second, Fourth, and Eighth Circuits have *rejected* a finding of standing on the particular facts of the cases heard in these circuits, while leaving the door open for future cases, noting that the assessment of risk of future harm is a fact-specific inquiry.[15] Conversely, the Third, Seventh, Ninth, and D.C. Circuits have held that, based on the facts of the particular cases, the risk of future harm from a data breach *was* an injury sufficient for standing.[16] The split regarding the existence of a cognizable injury centers around the risk of future identity theft, risk of future fraud, monitoring expenditures, and other similar costs.[17] Moreover, the Supreme Court has turned down the opportunity to opine on this subject, further solidifying the circuit split.[18]

---

8. *Id.*

9. 28 U.S.C. § 1332(d) (2011) (extending federal diversity jurisdiction to all class actions in which minimal diversity exists and the amount in controversy exceeds $5 million).

10. Megan Dowty, *Life is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 686 (2017).

11. *See* Balser et al., *supra* note 7.

12. *See* Balser et al., *supra* note 7.

13. David L. Silverman, *Developments in Data Security Breach Liability*, 74 BUS. L. 217, 217 (2018).

14. Dowty, *supra* note 10, at 686.

15. *See* Silverman, *supra* note 13; *see infra* Part II (discussing specific relevant cases from each circuit in the circuit split).

16. *See* sources cited *supra* note 15.

17. Dowty, *supra* note 10, at 686–87.

18. *See, e.g.*, Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

Some states, such as California, are passing stricter consumer privacy laws that will likely impact the future of data privacy litigation in those particular jurisdictions.[19] There have also been attempts to pass federal legislation that would potentially preempt state laws, but so far none of those attempts have succeeded.[20] Despite this lack of a clearly defined national standard, companies need to start employing techniques that will reduce their litigation exposure. Some options for accomplishing this include the implementation of a minimum level of security controls[21] and careful drafting of arbitration clauses and class action waivers[22] in the company's terms and conditions.

I. DATA BREACHES, IMPACT OF INFORMATION THEFT & CURRENT GOVERNING LAW

A. *Data Breaches: Prevalence Today & Resulting Costs to Victims*

As data breaches and hacks continue to occur, the privacy of our personal information remains constantly at risk, even if we believe the companies that we share our data with are trustworthy and technologically adept. Hackers continue to improve their skills and find new unpredictable methods of using technology to procure personal information from companies and individuals.[23] Unfortunately, the rate of technological development by these hackers seems to consistently outpace the policy makers in this area. This contributes to the general tensions on the subject and begs the question of why there has been so little progress in preventing data breaches and the thefts that often follow.[24] For example, in the last five years alone there have been several major corporate data breaches involving companies such as Target, Yahoo!, Home Depot, Sony Pictures and Entertainment, Anthem Health

19. *See generally* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2018).

20. *See* Stephen Jones, *Data Breaches, Bitcoin, and Blockchain Technology: A Modern Approach to the Data-Security Crisis*, 50 TEX. TECH. L. REV. 783, 793–94 (2018).

21. *See* KAMALA D. HARRIS, CAL. DEP'T OF JUST., CALIFORNIA DATA BREACH REPORT 31 (Feb. 2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

22. *See* Alexis Buese, *Calif. Privacy Law Will Likely Prompt Flood of Class Actions*, LAW360 (May 15, 2019, 11:41 AM), https://www.law360.com/articles/1159313/calif-privacy-law-will-likely-prompt-flood-of-class-actions.

23. *See* Jon L. Mills & Kelsey Harclerode, *Privacy, Mass Intrusion, and the Modern Data Breach*, 69 FLA. L. REV. 771, 773 (2017).

24. *Id.* at 773.

Insurance, HSBC Finance Corporation, Ashley Madison, and Equifax, just to name a few.[25]

Data breaches impact both the consumers whose records are exposed and the companies whose lack of appropriate security measures lead to the particular breach. The companies who are hacked, and ultimately leak such consumer information, are exposed to great financial harm.[26] The average cost to businesses per leaked record is reported at $150,[27] and the global cost of data breaches is estimated to increase to $2.1 trillion[28] by the end of 2019. These figures have consistently increased since 2017 and this trend may continue.[29] Further, customers with compromised credit card information or other personal data because of a data breach are often reluctant to do business with the same company, thus severing the relationship and resulting in the loss of a customer's lifetime value for the business.[30]

Repercussions on the consumer side typically center around the risk of future identity theft or fraud and the corresponding identity theft monitoring expenses, temporary account cancellations, and generalized stress and anxiety post-breach.[31] This is especially concerning given the general population's dependence on the Internet and will likely have the greatest impact on future generations. Future generations are at risk of serious identity theft issues that may occur when these individuals are still very young, which in turn may potentially impact their future ability to obtain loans or purchase homes, cars, and other valuable assets later in life that require an inquiry into credit scores.[32] All parties to a data breach suffer to some degree, and it is up to the policy-makers of the country to ultimately combat these issues by passing effective standards that will help protect future individuals from becoming victims of such harmful actions.

---

25. *Id.* at 780–83.

26. *See* Jones, *supra* note 20, at 789.

27. IBM SECURITY, COST OF A DATA BREACH REPORT 13 (2019), https://www.ibm.com/downloads/cas/ZBZLY7KL.

28. Shayla Price, *The Real Cost of Ecommerce Data Breaches, Espionage, and Security Mismanagement*, BIGCOMMERCE: ECOMMERCE SECURITY BLOG, https://www.bigcommerce.com/blog/data-breaches/#the-costs-of-a-data-breach (last visited Apr. 2, 2020).

29. IBM SECURITY, *supra* note 27, at 19.

30. *See* Price, *supra* note 28.

31. *See* Jones, *supra* note 20, at 788; Dowty, *supra* note 10, at 686; Price, *supra* note 28.

32. Jones, *supra* note 20, at 788–89; *see also* Danielle Wiener-Bronner, *Why Millennials Should be Really Worried about the Equifax Breach*, CNN MONEY (Sept. 15, 2017, 4:21 PM), https://money.cnn.com/2017/09/15/pf/millennials-equifax-breach/index.html.

B. *Impact of Information Theft: The Hacker's Timeline*

So, what actually happens after consumer personal information is stolen in a company's data breach? Hackers use the information in a variety of ways. They may: (1) use the stolen information to interfere with business operations, for example, hackers commonly sell internal business plans, forecasts, and market analyses to competitors; (2) steal data for the purposes of extortion, for example, ransomware attacks where the hacker demands payment if the company wants to unlock the stolen or restricted files; or (3) target consumer data like names, addresses, phone numbers, email addresses, passwords, credit card numbers, and social security numbers to leverage such information for financial gain on the dark web, which often results in identity theft that is sold to the highest bidder.[33] Of further concern, identity thieves often exploit stolen information within minutes of obtaining it.[34]

The Federal Trade Commission's Office of Technology Research & Investigation (FTC's Tech. Office) performed an experiment in 2017 to discover what actually happens when stolen personal information is made public and how quickly thieves attempt to make unauthorized use of the information.[35] The FTC's Tech. Office created personal information belonging to 100 fake people that was designed to look like a stolen database of consumer credentials and posted that information on a site frequented by hackers on two occasions.[36] For two weeks after they posted to the site, the FTC's Tech. Office monitored "all email access attempts, payment account access attempts, attempted credit card charges, and texts and calls received by phone numbers."[37] The first posting of information received about 100 views, and the second posting received about 550 views.[38] After the initial posting, it only took 90 minutes for the first unauthorized attempt to use the stolen fake information; then, after the second posting, it only took nine minutes.[39] Furthermore, the total number of attempts to use the information totaled

33. *See* Price, *supra* note 28.

34. *See* Lesley Fair, *Sensitive Consumer Data Posted Online (and the FTC Knows Who Did It)*, FEDERAL TRADE COMMISSION: BUS. BLOG (May 24, 2017, 10:30 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/05/sensitive-consumer-data-posted-online-ftc-knows-who-did-it.

35. *Id.*

36. *Id.*

37. *Id.*

38. *Id.*

39. *Id.*

119 in the first week and 1,108 in the second week.[40] Tracking of attempted illegal purchases over the two weeks lead to a variety of categories of charges, with the top five including: (1) retailers; (2) unknown; (3) gaming; (4) entertainment; and (5) e-payment services.[41]

The experiment revealed how incredibly fast large amounts of stolen personal information can spread across the dark web. The above experiment only used the data of 100 hypothetical victims of information theft and only tracked the impact for two weeks following the posting of the information. For a startling perspective, the Equifax data breach exposed personal information of approximately *147 million* individuals and that breach occurred two years ago in 2017.[42] The number of attempts of unauthorized use of such information from that one data breach alone is likely massive and will undoubtedly have a negative impact on the lives of those *real* breach victims.

C. *Current Data Breach Laws in the United States*

Federal data breach regulations are limited in their scope and apply almost exclusively to industries such as banking, finance, healthcare, and credit reporting.[43] Such statutes typically mandate that companies in each industry implement reasonable procedures to protect consumer information from prohibited disclosure.[44] Though this seems like a regulation that would result in something positive, it lacks any explanation or examples of what would qualify as "reasonable procedures" and it lacks guidance on how companies should assess their vulnerability for future data breaches.[45] The ambiguity of these federal statutes creates confusion and reinforces the wide array of security standards used nationwide, which are often effective.

If consumers recognize that they are victims of such statutory violations under the industry-specific federal law and bring a complaint against a company, they usually face an additional hurdle when arguing for federal standing and the interpretation of the injury requirement.[46] The

---

40. *Id.*

41. *Id.*

42. Lesley Fair, *$575 Million Equifax Settlement Illustrates Security Basics for Your Business*, FED. TRADE COMMISSION: BUS. BLOG (July 22, 2019, 6:48 AM), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/575-million-equifax-settlement-illustrates-security-basics.

43. Jones, *supra* note 20, at 792.

44. *See* Jones, *supra* note 20, at 792.

45. *See* Jones, *supra* note 20, at 792. *See also* 15 U.S.C. § 1681e(a).

46. *See infra* Section II.A.

Supreme Court of the United States has arrived at conflicting conclusions in regard to what actually satisfies this requirement, which has resulted in a federal circuit split.[47] Inevitably this adds to the outcome uncertainty for both plaintiffs and defendants, and since companies typically settle their disputes out of court,[48] courts have not been able to give opinions regarding their judgment on the merits of these claims. Notably, this impacts future litigation because the judicial system has not yet had the opportunity to interpret the meaning of what "reasonable procedures" should be in place to satisfy what is mandated by the federal statutes for protection of consumer personal information.

Every state (plus the District of Columbia and a number of United States Territories) has enacted legislation requiring entities to notify victims of security breaches that release personally identifiable information.[49] Each state's laws on security breaches usually set forth who must comply with the law, a definition of what constitutes "personally identifiable information" (which, surprisingly, varies state to state), what constitutes a breach, timing and appropriate method of notice, and certain exemptions.[50] Companies involved in a data breach are expected to comply with the various data-related statutes for each state where they do business.[51] However, the large range of varying regulations in this area, coupled with the added confusion related to standing present a burden for both the breached companies and the consumers seeking relief.[52]

Though data breach laws at the state level vary, they typically share the exception that notification is only required when compromised data was not encrypted (or when the encryption key was also compromised in the breach).[53] A number of state statutes require companies that collect consumer personal information to implement "reasonable procedures" to

47. Jones, *supra* note 20, at 794–95; *see* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 440–41 (2013) (suggesting a high burden of proof to meet the "certainly impeding" harm requirement); Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016) (holding that though the plaintiff alleged a federal statutory violation by the defendant, a concrete injury must also be shown); *see also infra* Section II.A.

48. *See* Jones, *supra* note 20, at 793.

49. *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Sept. 29, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/ security-breach-notification-laws.aspx [hereinafter NCSL].

50. *Id.*

51. Jones, *supra* note 20, at 791–92; *see generally* NCSL, *supra* note 49 (showing the varying statutes related to this subject for each state).

52. *See* Jones, *supra* note 20, at 792.

53. Jones, *supra* note 20, at 796.

protect the information.[54] However, similar to the federal statutes that require such "reasonable procedures," the state laws do not provide any guidance regarding the types of procedures considered reasonable and they also do not shed light on how companies should assess their vulnerability for future data breaches.[55] And the most notable differences across the state statutes are how broad or narrow they define "personal information," whether they provide consumers with an express cause of action, the severity of the penalties for violations, and the range of time that breached companies have to notify consumers and regulatory agencies of the breach.[56]

The state of Florida's data and personal information protection statutes are typical examples of what any state statutes may look like in this area. These data breach laws apply to any entity that acquires, maintains, stores, or uses personal information.[57] Entities are required to take "reasonable measures" to protect and secure data in electronic form containing personal information.[58] The statute defines "breach of security" or "breach" as unauthorized access of data in electronic form containing personal information, with an exception for certain situations where information is accessed in good faith by employees or agents.[59] It does not apply to encrypted or redacted information, or information secured in some other way that renders it unreadable (as long as the encryption key is not also compromised).[60] Within the statute "personal information" is defined as an individual's first and last name or first initial and last name plus one or more of the following: Social Security number, driver's license or passport number, military identification number, any similar form of government identification number that can be used to verify the individual's identity, financial account number or credit or debit card number with any security codes required, medical information, or health insurance policies or subscriber identification numbers.[61] Additionally, personal information may also include a username or e-mail address, in combination with a password or security question and answer

54. Jones, *supra* note 20, at 796–97.

55. Jones, *supra* note 20, at 797.

56. Jones, *supra* note 20, at 796–97.

57. FLA. STAT. § 501.171(1)(b) (2019).

58. *Id.* § 501.171(2). The vague "reasonable measures" language, *id.*, provides little guidance to businesses for best prevention practices.

59. *Id.* § 501.171(1)(a).

60. *Id.* § 501.171(1)(g)(2).

61. *Id.* § 501.171(1)(g)(1)(a).

that would permit access to an online account.[62] Florida's statute does not provide a private cause of action.[63]

Florida's notification requirement varies depending on whether the breached entity is notifying an individual or a regulatory agency.[64] For individuals, notifications must be given in writing to each individual in the state whose personal information was, or if the entity reasonably believes it was, accessed as a result of the breach.[65] The notice shall be made "as expeditiously as practicable and without unreasonable delay . . . but no later than 30 days after the determination of the breach or reason to believe the breach occurred" and must include the date(s) of the breach, a description of the personal information accessed or believed to be accessed, and contact information for the breached entity.[66] For regulators, the breached entity must notify the Florida Department of Legal Affairs no later than 30 days following the identification of the breach if 500 or more individuals within the state are affected by the breach.[67] Further, third parties that maintain personal information on behalf of the breached entity must notify that entity no later than 10 days after determination of the breach.[68] Violations of the notice requirement may result in civil penalties and are considered "unfair or deceptive trade practices."[69] The civil penalties may consist of up to $1,000 per day for each day up to the first 30 days following a violation and $50,000 for each subsequent 30-day period or portion thereof for up to 180 days, capping at a ceiling of $500,000.[70] These penalties are per breach, not per affected individual.[71]

The difficulties that both consumers and businesses must overcome from the current data breach regulations on the federal and state levels are clear. Unfortunately, the subsequent path going forward after overcoming those difficulties is not so clear. The following sections of this Article summarize and examine the split among the federal circuit courts, the forthcoming state regulations that will likely have a substantial impact on data protection laws across the country, and the potential

62. *Id.* § 501.171(1)(g)(1)(b).
63. *Id.* § 501.171(10).
64. *Compare* FLA. STAT. § 501.171(3), *with* FLA. STAT. § 501.171(4).
65. *Id.* § 501.171(4)(a), (d).
66. *Id.* § 501.171(4)(a), (e).
67. *Id.* § 501.171(3)(a). Fifteen additional days may be allowed if there is good cause for delay provided in writing to the department within 30 days after determination of the breach or reason to believe a breach occurred. *Id.*
68. *Id.* § 501.171(6)(a).
69. *Id.* § 501.171(9)(a).
70. *Id.* § 501.171(9)(b).
71. *Id.* § 501.171(9).

measures that companies can implement to mitigate their litigation exposure in this area.

II. A SPLIT AMONG THE CIRCUIT COURTS

Data breach cases typically include one or more of three different categories of alleged injuries: (1) the plaintiff's personal or financial information has been stolen by a third party, and that party has used that information illegally (i.e. to make purchases using the plaintiff's money); (2) the plaintiff's information has been accessed but that information has not been used (i.e. to open bank accounts, make unauthorized purchases, or otherwise harm the plaintiff), yet, the plaintiff still claims other forms of damages (i.e. incurring costs for credit-monitoring services, paying the cost of cancelling and receiving new bank bards, suffering loss of reward points from cancelled cards, and experiencing general anxiety that their information will be used in an unauthorized manner in the future); and (3) the plaintiff brings a suit based on a belief that his information is not being protected and a third party could potentially access it in the future.[72] From these above categories of injuries, those in (1) involve an injury sufficient to meet the injury-in-fact requirement, those in (2) are the type of injuries involved in the circuit split that focuses on whether the indirect costs and expenses are sufficient to meet the injury-in-fact requirement, and those in (3) are the least likely to meet the injury-in-fact requirement.[73]

The lack of a uniform standard set by the Supreme Court for what constitutes injury in the context of data breaches has resulted in a circuit split as to how much injury is sufficient for standing purposes. Generally, the First, Second, Fourth, and Eighth Circuits have consistently *rejected* a finding of standing for alleged injury categories (2) and (3) above, while emphasizing that the assessment of risk of future harm is a fact-specific inquiry.[74] Conversely, the Third, Seventh, Ninth, and D.C. Circuits have consistently held that the alleged injury category (2)—risk of future harm from a data breach that has already occurred—*was* an injury sufficient for standing.[75]

---

72. Caroline C. Cease, Note, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395, 398, 399, 404 (2014).

73. *Id.* at 398, 399, 404.

74. Silverman, *supra* note 13, at 217.

75. Silverman, *supra* note 13, at 217.

A. *First Things First: Standing*

1. The "Injury-in-Fact" Requirement

The Constitution establishes Article III standing as a "threshold question in every federal court case."[76] To satisfy this standing requirement, a plaintiff must have suffered an injury that is: (1) concrete, particularized and actual or imminent (as opposed to merely conjectural or hypothetical); (2) fairly traceable to the challenged conduct of the defendant; and (3) likely to be redressed by a favorable ruling.[77] Standing issues for data breach cases usually center around the first requirement—that there is an "injury-in-fact." However, the Supreme Court has not yet directly ruled on this subject in the context of a data breach.

Many data breach cases addressed by lower courts have relied on *Clapper v. Amnesty International USA* for guidance on analyzing the existence of a sufficient injury-in-fact.[78] *Clapper* involved a United States citizen who engaged in sensitive international communications with individuals whom they believed might be the targets of American surveillance at some point in the future under the 2008 Amendments to the Foreign Intelligence Surveillance Act.[79] The plaintiffs claimed to have suffered an injury-in-fact because of a reasonable likelihood that their communications with foreign contacts would be intercepted, and because the risk of surveillance required them to take costly and burdensome actions to protect the confidentiality of their communications.[80] However, there was no evidence that the plaintiffs' communications had been targeted or that the government was going to target their communications in the future.[81]

As a result, the Court held in a 5-4 decision that the plaintiffs did not have standing under Article III.[82] The Court "reiterated that [the] 'threatened injury must be *certainly impending* to constitute injury-in-fact,' and that '[a]llegations of *possible* future injury' are not sufficient."[83] Specifically, the Court found that plaintiffs' theory of future injury was "too speculative," and not actual or "certainly impending," with the plaintiffs' allegations for standing based on a "highly attenuated

76. United States v. One Lincoln Navigator 1998, 328 F.3d 1011, 1013 (8th Cir. 2003).
77. Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010).
78. *See generally* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).
79. *Id.* at 401–05.
80. *Id.* at 401.
81. *Id.* at 411.
82. *Id.*
83. *Id.* at 409 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

chain of possibilities."[84] Further, the Court found that plaintiffs' "contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm [was] unavailing . . . [because they] cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[85]

Since *Clapper*, cases have been inconsistent on the issue of Article III standing and the injury-in-fact requirement. The injury-in-fact analysis is very fact-specific in nature, with some courts finding no standing on imminence grounds, reasoning that the plaintiff had suffered no actual injury, while others find standing in cases involving similar facts and claims. In fact, there are several notable data breach and privacy class action cases that have contributed to this split of authority.

2. Circuits Finding Injury Sufficient for Standing: Third, Sixth, Seventh, Ninth, & D.C.

In the Third Circuit, the decision in *In re Horizon* involved two stolen laptops that contained unencrypted personal information (specifically, health insurance data, names, addresses, dates of birth, and social security numbers) of more than 839,000 Horizon members.[86] Of those with information stolen, only one named plaintiff experienced *actual* misuse in the form of a fraudulent tax filing.[87] The plaintiffs alleged willful and negligent violations of the Fair Credit Reporting Act and numerous violations of state law, centering around Horizon's failure to take reasonable and appropriate measures to secure the stolen laptops and safeguard the member's information.[88] In its opinion, the court clarified the standing requirements for plaintiffs asserting violations of certain federal statutes.[89]

The court held that the plaintiffs, by alleging an unauthorized transfer of personal identifying information in violation of the Fair Credit Reporting Act, had established a sufficient *de facto* injury for standing, even if that information was not improperly used.[90] This decision narrowed the lack of standing defense in this particular type of data

84. *Id.* at 401, 410.

85. *Id.* at 415.

86. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 630 (3d Cir. 2017).

87. *Id.*

88. *Id.* at 629, 631.

89. *Id*. at 639–40.

90. *Id.* at 629, 636.

breach case, where the claim involved arose from certain statutory rights. However, the result still leaves open whether other federal statutes may recognize data breaches as injuries-in-fact, and whether more technical violations of statutes could constitute a harm for standing.

In the Sixth Circuit, the data breach in *Galaria v. Nationwide Mutual Insurance Co.*, involved the theft of personal information (specifically, names, dates of birth, driver's license numbers, and social security numbers) of 1.1 million customers of Nationwide Mutual Insurance Company by hackers of the company's computer network.[91] Plaintiffs sued Nationwide for violating the Fair Credit Reporting Act (failure to adopt adequate procedures to protect personal information) and for common law torts of negligence and bailment.[92] Plaintiffs alleged that they had incurred costs associated with mitigating the risk, including purchasing credit reporting and monitoring services for credit reports and bank statements.[93] Ultimately, a split panel held that plaintiffs had sufficiently demonstrated standing by alleging that the Nationwide hack had subjected them to significantly heightened risk of fraud and identity theft.[94]

The court found that even though plaintiffs claimed no incidences of actual fraud or identity theft, their claimed injury was not merely "hypothetical."[95] The court reasoned, while distinguishing the facts of this case from those in *Clapper*, "[t]here is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals. . . . Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for . . . fraudulent purposes."[96] Further, the court also noted that Nationwide seemed to recognize the severity of the risk because it offered free credit monitoring and identity theft protection for one year; thus Nationwide's mitigation efforts were actually used against them in the end.[97] This decision is one of the most favorable to plaintiffs in the data breach context because no plaintiffs even alleged any actual fraud or identity theft as a result of the data theft.

In the Seventh Circuit, the data breach in *Remijas* involved hackers attacking Neiman Marcus and stealing the credit card numbers of

91. Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 386 (6th Cir. 2016).
92. *Id.*
93. *Id.* at 386–87.
94. *Id.* at 388.
95. *Id.*
96. *Id.*
97. *Id.*

approximately 350,000 of its customers.[98] Some of these customers found fraudulent charges on their cards around the same time of the breach.[99] The court asserted that *Clapper* did not consummately bar consumers from bringing suit based on substantial risk of future injury and found that the costs incurred by the plaintiffs were material enough to be considered particularized injuries.[100] Neiman Marcus' major objection was that the plaintiffs could not show that their injuries were fairly traceable to the Neiman Marcus breach instead of a breach involving Target, which occurred around the same time.[101] The court responded by stating that, "if there are multiple companies that could have exposed the plaintiffs' private information to hackers, then the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury."[102] The court ultimately held that "injuries associated with resolving fraudulent charges and protecting oneself against future identity theft" were sufficient to confer Article III standing.[103]

In the Ninth Circuit, the data breach in *Krottner v. Starbucks Corp.* involved the theft of a laptop containing the personal information (specifically, names, addresses, and social security numbers) of Starbucks employees.[104] While the leaked information had not yet been misused, the plaintiff's sued Starbucks for negligence and breach of implied contract, emphasizing that the data leaked had increased their risk of identity theft.[105] Here, the court asserted that plaintiffs alleged "a credible threat of real and immediate harm stemming from the theft of the laptop containing their unencrypted personal data."[106] It explained that had the allegation been more conjectural or hypothetical (i.e., if no laptop had been stolen and the plaintiffs sued based on the risk that it would be stolen in the future), the threat would be much less credible.[107] Thus, plaintiff's satisfied the injury-in-fact requirement for Article III standing by stating that an injury-in-fact can be satisfied by a threat of future harm, or by an act which harms the plaintiff only by increasing the risk of future

98. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 689–90 (7th Cir. 2015).
99. *Id.*
100. *Id.* at 694.
101. *Id.* at 696.
102. *Id.*
103. *Id.*
104. Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010).
105. *Id.* at 1140–41.
106. *Id*. at 1143.
107. *Id.*

harm that plaintiff would have otherwise faced, absent defendant's actions.[108]

Though *Krottner* occurred before the Supreme Court's decision in *Clapper*, the Ninth Circuit subsequently decided another data breach case in *In re Zappos.com, Inc.*, where it reiterated its expansive view of injuries involving the risk of future harm for standing.[109] In that case, the court unanimously held that plaintiffs, whose personal information (specifically, payment card data) was stolen but not actually misused, had standing to sue because they faced a substantial risk of identity theft.[110] This is important because it held that *Krottner* is still good law after the decision in *Clapper*.[111]

Finally, in the D.C. Circuit, the data breach in *Attias v. CareFirst, Inc.* involved a cyberattack where 1 million CareFirst's customers' personal information (specifically, names, dates of birth, email addresses, and subscriber information) was stolen.[112] Plaintiffs argued that CareFirst violated state laws and legal duties by failing to safeguard their information and exposing them to an increased risk of identity theft.[113] The court stated that this injury was sufficient to establish standing because it was "at the very least . . . plausible" to infer that the hackers had the intent and ability to use the stolen data for illegal purposes.[114]

The above cases from this side of the circuit split present the hurdles a defendant must clear to secure dismissal of a data breach claim. Generally, they collectively held that the risk of future harm from a data breach was, on its face, injury sufficient for standing. Based on these plaintiff-favorable rulings on the standing issue, these circuits will likely emerge as the forums of choice for data breach class actions. And as the Supreme Court recently denied *certiorari* in 2018 for *CareFirst*, this split remains in place for the foreseeable future.

3. Circuits Finding No Injury Sufficient for Standing: First, Second, Fourth, & Eighth

In the First Circuit, the case of *Katz v. Pershing* involved a unique set of facts in this context because the case was actually filed before any data

108. *Id.*
109. *In re* Zappos.com, Inc., 888 F.3d 1020, 1030 (9th Cir. 2018).
110. *Id.* at 1023, 1030.
111. *Id*. at 1023.
112. Attias v. CareFirst, Inc., 865 F.3d 620, 622–23 (D.C. Cir. 2017), 865 F.3d at 622.
113. *Id*. at 623.
114. *Id.* at 628.

breach occurred.[115] Plaintiff alleged that she experienced an increased risk of potential future loss due to the defendant's alleged failure to adhere to reasonable security practices and privacy regulations.[116] The court held that such allegations were not sufficient to meet the requirements for Article III standing.[117] It reasoned that the allegations of harm were too speculative and could not show impending injury because the facts alleged left too many unknown variables, including whether the plaintiff's data would actually be stolen or lost, and even then, whether the data would be misused in a way that would harm her.[118] Ultimately, the plaintiff's standing theory rested "entirely on the hypothesis that at some point an unauthorized, as-yet unidentified, third party might access her data and then attempt to purloin her identity."[119]

In the Second Circuit, the data breach in *Whalen v. Michaels Stores, Inc.* involved the theft of customers' credit card and debit card data (specifically, card numbers and expiration dates).[120] Relying on the standard from *Clapper*, the court deemed the named plaintiff's allegation of two attempted fraudulent credit card charges insufficient to make the risk of future harm "certainly impending."[121] Because plaintiff was never asked to pay, nor did she pay, any fraudulent charges and because her stolen credit card was promptly canceled after the breach and no other personally identifying information (such as her date of birth or social security number) was alleged to have been stolen, the court concluded that she had alleged no injury that would satisfy the constitutional standing requirements of Article III.[122]

In the Fourth Circuit, *Beck v. McDonald* consolidated two cases against a Veteran's hospital.[123] The first involved a stolen laptop with limited data (specifically, names, dates of birth, last four digits of social security numbers, and physical descriptors) and the second involved stolen boxes of pathology files with information (specifically, names, social security numbers, and medical diagnoses) about deceased persons.[124] Interestingly, the court denied standing for both sets of facts,

115. Katz v. Pershing, LLC, 672 F.3d 64, 64 (1st Cir. 2012).
116. *Id.* at 78.
117. *Id.* at 80–81.
118. *Id.* at 80.
119. *Id.* at 79.
120. Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017).
121. *Id.*
122. *Id.* at 90–91.
123. Beck v. McDonald, 848 F.3d 262, 266 (4th Cir. 2017).
124. *Id.* at 267, 268.

but adopted the reasoning from *Krottner* and *Remijas* (which, as explained above, are on the opposite side of the circuit split), implying that some breaches do make future harm certainly impending.[125] Ultimately, it seems that, for this specific case, the fact that three years had passed without any visible misuse of the personal information proved decisive and the court found that the threat of identity theft stemming from these breaches was too speculative to establish an injury-in-fact for these claims.[126]

In the Eighth Circuit, *In re SuperValu, Inc.* involved two data breaches on a chain of retail grocery stores in which hackers gained access to the payment information of customers (specifically, names, credit or debit card numbers, card expiration dates, card verification value codes, and personal identification numbers).[127] The plaintiffs alleged that the defendant failed to take adequate measures to protect customers' information; for example, the defendant allegedly used default or common passwords, failing to lock out users after several failed login attempts and not segregating access to different parts of the computer network or use firewalls to protect customer information.[128] The plaintiffs claimed that customer information was stolen as a result of the breaches, subjecting plaintiffs to "an imminent and real possibility of identity theft."[129] One plaintiff also alleged that he suffered a fraudulent charge on his credit card statement, resulting in the replacement of the card.[130] In the end, however, the court found that the individual plaintiffs who had not experienced any fraudulent charges or identity theft following the breaches and had not sufficiently alleged a substantial risk of future injury.[131] But the court did find that the injury of the one plaintiff who alleged fraudulent use of this card gave rise to standing in his individual case.[132]

The above cases from this side of the circuit split have generally held that plaintiffs must allege an actual injury in the form of fraudulent charges on existing credit or debit card accounts or the opening of fraudulent financial accounts resulting from their stolen personal information to establish the requisite injury-in-fact for Article III

125. *Id.* at 273, 274.
126. *Id.* at 274–75.
127. *In re* SuperValu, Inc., 870 F.3d 763, 766 (8th Cir. 2017).
128. *Id.*
129. *Id.*
130. *Id.* at 767.
131. *Id.* at 771–72.
132. *Id.* at 774.

standing. They have determined that general allegations of a heightened risk of identity theft from stolen personal information alone do not constitute an injury-in-fact, raising the pleading requirements for plaintiffs in data breach cases in these jurisdictions. Thus, with the circuit split firmly in place, the potential for standing will largely depend on both where the suit is filed and on that court's interpretation of the standard to prove sufficient standing.[133]

B. *Next Step: Causation & Redressability*

For those cases that are fortunate enough based on their particular factual situations to make it past the first hurdle of injury-in-fact for Article III standing, the next challenge presented focuses on causation and redressability. The data breach context presents a somewhat unique circumstance surrounding causation (typically meaning that the injury must be fairly traceable) because of the ability of a data thief to aggregate data from multiple sources. This creates issues for courts who enforce a strict "rule of enablement," which means that the data stolen must have been sufficient by itself to enable the alleged misuse.[134] And while forensic testing may reveal how a breach was achieved and what data was stolen, such evidence-based results seldom exist to prove a direct connection between the act of the breach and a particular subsequent misuse that resulted in injury.[135]

As noted by the court in *Remijas* above, once a set of mostly immutable personal information has been involved in multiple breaches, causation becomes an even harder element to prove.[136] Courts have approached this issue in different ways. Most notable from a public policy standpoint was that of *In re Yahoo! Inc. Customer Data Security Breach Litigation*, where the court "refused to consider that any instances of actual misuse might have resulted from other data breaches, as this would create a perverse incentive for stewards of consumer data."[137] But some courts analyzing data breach cases deem that this standing requirement has been satisfied where a business admits customer information has been exposed by issuing data breach notifications (as they are legally required to give such notifications under state privacy laws) or where a business

133. *See* Cease, *supra* note 72, at 404.

134. *See* David L. Silverman, *Developments in Data Security Breach Liability*, 73 BUS. LAW. 215, 218–19 (2017) [hereinafter 2017 Data Breach Developments].

135. *See* Silverman, *supra* note 13, at 221.

136. *See* Silverman, *supra* note 13, at 221–22.

137. *See* Silverman, *supra* note 13, at 222.

issues new customer cards themselves due to a breach.[138] Ultimately, some courts are more reluctant than others to recognize causation, so jurisdiction choice will also impact this outcome regarding the standing determination.

Redressability is the final step in the Article III standing analysis, and it has been invoked the least often in data breach cases.[139] The injurious standard to satisfy is that "it must be likely, as opposed to merely speculative, that [an] injury will be redressed by a favorable decision."[140] Major issues in this area typically center around failures to allege any quantifiable damages resulting from the breach and instances where credit card companies or other parties have already remedied some of the victims' injuries.[141] If these issues are present, the plaintiffs' claimed injuries may struggle to pass the test for redressability.

III. ATTEMPTS AT A FEDERAL STANDARD & FORTHCOMING STATE LEGISLATION

Though there have been a number of attempts at passing a uniform federal standard, the United States lacks a comprehensive federal law that regulates the collection and use of consumer personal information. As a result, many states have passed their own laws, which often contain different and sometimes incompatible provisions regarding what categories and types of personal information are protected or which entities are covered. In addition, the judicial circuits have also diverted from a single interpretation in the data breach standing context, which only adds to the inconsistency and confusion across the board. Congress's ability to successfully pass a uniform federal data breach standard is highly dependent on the political state of the country, and with the current stark divide surrounding political views on the subject of federal regulation, such a federal standard is not likely to be enacted anytime soon. Fortunately, California's new privacy regulation possesses the potential to cause a seismic shift in the landscape of data privacy law, not just in California, but across the country.

138. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696 (7th Cir. 2015); *In re* Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 487 (D. Minn. 2015).

139. *See* 2017 Data Breach Developments, *supra* note 134, at 220.

140. Lujan v. Defs. Of Wildlife, 504 U.S. 555, 561 (1992).

141. *See, e.g.*, Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 857 (S.D. Tex. 2015).

A. *Attempts at a Federal Standard*

Many have called on Congress to enact flexible and technologically neutral privacy and security laws. For example, in 2014, the "Data Security Breach Notification Act" was introduced in the Senate; however, it did not move past referral to a Senate subcommittee.[142] Then, the Barack Obama presidential administration put forth plans in 2015 for the "Personal Data Notification & Protection Act," which proposed many measures aimed at promoting data security, data privacy, and protection against identity theft, including a "Consumer Privacy Bill of Rights."[143] This was largely based on the Fair Information Practice Principles, which are thought of as general processes and procedures that organizations should implement, recognizing that Americans have a strong interest in how information about them is collected, used, and shared by companies.[144]

The 2015 Act aimed to protect "sensitive personally identifiable information," including: (1) first and last name in combination with several different elements; (2) a government-issued identification number, including a social security number or driver's license number; (3) biometric data including fingerprints or voice prints; (4) unique account identifiers; and (5) a username in combination with a password or security question.[145] It also contained a strict standard of notification requirements which would have been enforced by the Federal Trade Commission and state Attorney Generals.[146] A major point of contention in this bill was that the Personal Data Notification & Protection Act would supersede any state laws covering breaches of computerized data from businesses.[147] Unfortunately, this proposal lost momentum shortly after a draft of the bill was put forward and it also did not move past subcommittee review.[148] Most recently, the Donald J. Trump presidential

142. *See* Martha Wrangham & Gretchen A. Ramos, *Calls for Federal Breach Notification Law Continue After Yahoo Data Breach*, THE NAT'L L. REV. (Oct. 5, 2016), https://www.natlawreview.com/article/calls-federal-breach-notification-law-continue-after-yahoo-data-breach.

143. *See* OFFICE OF THE PRESS SEC'Y, FACT SHEET: SAFEGUARDING AMERICAN CONSUMERS & FAMILIES (Jan. 12, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families.

144. *See* Brendan McDermid, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

145. Personal Data Notification & Protection Act, H.R. 1704, 114th Cong. § 112(12) (2015).

146. *Id.* at § 101(c); *see also id.* §§ 107–108 (explaining the rules and methods of enforcement).

147. *See id.* § 109.

148. *See* Wrangham & Ramos, *supra* note 142.

administration's lack of appetite for technology policy or regulation in general has left this issue and any attempts at a federal data breach standard at a standstill for the foreseeable future.[149]

B. *The California Consumer Privacy Act*

California has always had a strong policy regarding the subject of privacy, often enumerating more elaborate and stricter privacy laws than other states. In fact, California even enumerated the right to privacy in its constitution.[150] Once again, California is charging forward in the world of privacy legislation and on June 28, 2018, with subsequent minor amendments, it has enacted the California Consumer Privacy Act (CCPA).[151] The CCPA will go into effect starting January 1, 2020, and it will generally restrict certain businesses' ability to collect and sell the "personal information" of consumers.[152] Though the CCPA will take effect in a single state, its reach will extend well beyond the borders of California, and its expansive protections mark a major shift in the nation's data privacy regime.[153]

The CCPA applies to any for-profit business (regardless of where it is located) that collects the personal information of California residents and satisfies at least one of the following criteria:

> (1) generates gross revenues above $25 million (and such threshold is not limited to revenue earned in the State of California), (2) engages in the buying, selling, receiving, or sharing of the personal information of at least 50,000 California residents, households, or internet-connected devices, or (3) derives at least 50% of its annual revenues from the sale of consumers' personal information.[154]

The definition of this type of business for purposes of the CCPA also includes "[a]ny entity that controls or is controlled by a business, as

149. *See* McDermid, *supra* note 144.

150. CAL. CONST. art I, § 1 (providing that "[a]ll people are by nature free and independent and have inalienable rights . . . enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy").

151. *See* WILSON C. FREEMAN, CONG. RESEARCH SERV.: LEGAL SIDEBAR, CALIFORNIA DREAMIN' OF PRIVACY REGULATION: THE CALIFORNIA CONSUMER PRIVACY ACT AND CONGRESS 1 (Nov. 1, 2018).

152. *See* CAL. CIV. CODE § 1798.105.

153. *See* FREEMAN, *supra* note 151.

154. CAL. CIV. CODE § 1798.140(c)(1).

defined in [the main "business" definition], and that shares common branding with the business.[155]

The CCPA also contains a limited number of exemptions to the definition of "business." If every aspect of the commercial conduct takes place wholly outside of California, then such business is exempt from the CCPA.[156] Also exempted from its coverage is the collection of certain information covered by other statutes, including HIPAA, the FCRA, the GLBA, and the DPPA, as well as "publicly available information," which includes information lawfully made available from government records.[157] The CCPA's definition of "personal information" is very inclusive, encompassing all "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[158]

---

155. *Id.* § 1798.140(c)(2).

156. *Id.* § 1798.145(a)(6).

157. *Id.* § 1798.145. *See also* FREEMAN, *supra* note 151, at 2.

158. *Id.* § 1798.140(o)(1). The CCPA includes examples of what is included in the definition of "personal information":

> (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
>
> (B) Any categories of personal information described in subdivision (e) of Section 1798.80.
>
> (C) Characteristics of protected classifications under California or federal law.
>
> (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
>
> (E) Biometric information.
>
> (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.
>
> (G) Geolocation data.
>
> (H) Audio, electronic, visual, thermal, olfactory, or similar information.
>
> (I) Professional or employment-related information.
>
> (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights

Such a broad definition illustrates the intent of the CCPA's drafters regarding the statute's breath and its ability to provide expansive protections to consumers.[159] And ultimately, even with the exemptions, these provisions will likely reach a considerable number of businesses with a website accessible in California.

The CCPA confers three major "rights" on consumers: the "right to know," the "right to opt out," and the "right to delete."[160] The "right to know" is derived from the fact that businesses must, in advance of any collection, "inform consumers [by mail or electronically] as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used."[161] Further, in addition to requiring this advance collection disclosure, consumers also have the right to request that a business that collects personal information about the consumer disclose to the consumer the specific pieces of personal information that the business has collected or sold from the consumer, the categories of sources from which the information was collected, the business purposes for collecting or selling the personal information, and the third parties with whom the information was shared.[162]

Next, the "right to opt out" derives from the requirement that businesses must inform consumers of the right to opt out of the sale of a consumer's information, and if a consumer so directs a business not to sell the consumer's personal information, the business cannot again sell the consumer's information unless the consumer subsequently provides the business express authorization.[163] It also requires an affirmative "opt

---

and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. *Id.*

159. *See* FREEMAN, *supra* note 151, at 3.

160. *See* CAL. CIV. CODE §§ 1798.100, 1798.120, 1798.105.

161. *Id.* § 1798.100(b). This information will be provided to the consumer free of charge. *Id.* § 1798.100(d).

162. *Id.* § 1798.110(a).

163. *Id.* § 1798.120. With respect to the "right to opt-out," businesses must provide a "clear and conspicuous link" on their homepage entitled "Do Not Sell My Personal Information" that opens an Internet Web page enabling a consumer to opt-out of the sale of the consumer's personal information. *Id.* § 1798.135(a)(1). Additionally, the business must also include a description of consumers' opt-out rights, along with a separate link to the "Do Not Sell My Personal Information" webpage in its online privacy policy. *Id.* § 1798.135(a)(2).

in" for consumers under the age of 16 (by the consumer directly if they are between the ages of 13 and 16 or by the consumer's parent of guardian if the consumer is under 13).[164] Finally, the "right to delete" derives from the requirement that businesses, if requested by a consumer, must delete any information collected about such consumer.[165] The CCPA provides some exceptions to this right, including: when the information is needed to complete a particular transaction for the consumer, to detect security incidents or protect against fraud, or where such retention enables solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.[166]

As an additional protection for consumers, the CCPA contains a nondiscrimination rule to backstop the discussed rights. Specifically, it provides that no business may discriminate against a consumer by "denying goods or services," by "charging different prices or rates," or by "providing a different level or quality of goods or services" to consumers who exercise their rights under the CCPA.[167] However, the CCPA *does* allow businesses to "offer financial incentives" for the collection, sale, or non-deletion of personal information. It also provides that a business may offer a different price to consumers who exercise their rights "if that price . . . is directly related to the value provided to the consumer by the consumer's data."[168]

Enforcement of the CCPA will largely fall under the authority of the California Attorney General. Businesses that are in violation of the CCPA and do not cure those violations within 30 days are liable for civil penalties of up to $2,500 for each violation, which increases to $7,500 if the violation is intentional.[169] Moreover, it gives California residents a civil right of action for injunctive or declaratory relief, as well as monetary damages (no less than $100 and no more than $750 per incident, or actual damages, whichever is greater) against businesses that fail to implement *reasonable security measures* to protect their personal information.[170] Significantly, "reasonable security measures" are not defined by the CCPA, and in the absence of a specified definition, a definition will likely be determined by the judicial system and analyzed

164. *Id.* § 1798.120(d).

165. *Id.* § 1798.105. Following such a request, the business must delete the information from its own records, as well as the records of it service providers. *Id.* § 1798.105(c).

166. *Id.* § 1798.105(d).

167. *Id.* § 1798.125(a)(1).

168. *Id.* §§ 1798.125(b)(1), (a)(2).

169. *Id.* § 1798.155(b).

170. *Id.* § 1798.150(a)(1).

on a case-by-case basis. Such actions can only be brought if a consumer provides a business with 30 days' written notice and provides the business with the opportunity to "cure" the violation, unless the consumer suffered actual pecuniary damages.[171] This safe harbor cuts both ways: on the one hand, it will provide business with advance notice of the claims and the ability to engage plaintiffs before litigation progresses; and on the other hand, because of the uncertainty in the statute as drafted (i.e., how to "cure" is not defined), it is not clear what an actual cure of a data breach would look like.[172]

Overall, the CCPA will regulate how businesses with an online presence in California collect, share, and use consumer personal information. This unprecedented change in California's privacy law will invite an explosion of consumer litigation as plaintiffs seek to recover statutory damages under the private right of action.[173] Whereas thus far, plaintiffs have often struggled to sufficiently demonstrate that theft of their data has resulted in an injury-in-fact for standing purposes, the new allowance for statutory damages has cleared a major litigation hurdle for plaintiffs since they will no longer need to demonstrate that an actual financial injury has been suffered.[174] It is very likely that because of its expansive scope and jurisdictional reach, the CCPA will become the standard for best practices in privacy and data protection for United States residents unless it is later preempted by federal law, or another state adopts a law with more demanding requirements.

IV. POTENTIAL MITIGATION OF LITIGATION EXPOSURE

The best chance for avoiding litigation exposure from the company's perspective, is to implement adequate security measures to prevent data breaches in the first place. As previously stated, the federal and state data security statutes generally require that companies in possession of customer personal information implement adequate security measures, though they do not offer any further explanation of what would qualify or how such companies should assess vulnerabilities. For some guidance on this matter, the Center for Internet Security's Critical Security Controls identifies a minimum level of information security that all organizations that collect or maintain personal information should meet in order to meet the standard for reasonable security.[175] The minimum security controls for effective cyber defense are listed below.[176]

171. *Id.* § 1798.150(b).
172. *See* Buese, *supra* note 22.
173. *See* Buese, *supra* note 22.
174. *See* Buese, *supra* note 22.
175. *See* HARRIS, *supra* note 21, at 30.
176. *See* HARRIS, *supra* note 21, app. at 39.

CSC 1 Inventory of Authorized and Unauthorized Devices
CSC 2 Inventory of Authorized and Unauthorized Software
CSC 3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC 4 Continuous Vulnerability Assessment and Remediation
CSC 5 Controlled Use of Administrative Privileges
CSC 6 Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7 Email and Web Browser Protection
CSC 8 Malware Defenses
CSC 9 Limitation and Control of Network Ports, Protocols, and Services
CSC 10 Data Recovery Capability
CSC 11 Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12 Boundary Defense
CSC 13 Data Protection
CSC 14 Controlled Access Based on the Need to Know
CSC 15 Wireless Access Control
CSC 16 Account Monitoring and Control
CSC 17 Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18 Application Software Security
CSC 19 Incident Response and Management
CSC 20 Penetration Tests and Red Team Exercises

These controls should serve as a starting point, and the failure to implement all twenty that apply to a particular company's data environment could constitute a lack of reasonable security.[177]

Further, companies should make multi-factor authentication available on consumer-facing online accounts that contain sensitive personal information, such as requiring something biometric (i.e., a fingerprint) or an additional code to enter that comes through as a text or other one-time-password token.[178] Such requirements would make it much more difficult for a third party to breach the account because access to the account would require more than just the baseline username and password combination. Companies are also well advised to consistently use strong

177. *See* HARRIS, *supra* note 21, at 30.

178. *See* HARRIS, *supra* note 21, at 34–35.

encryption methods to protect personal information on mobile electronic devices (such as laptop computers or smart phones) that could be physically lost or stolen.[179] Ultimately, in this context the motto really is "better safe than sorry." When in doubt it is better to implement as many security controls as are feasibly possible for the particular type and size of the company, based upon the sensitivity of the stored personal information.

Additional methods for reducing a company's litigation exposure incorporate the use of an arbitration clause and a class action waiver in the website's terms and conditions, which could prohibit users from prompting mass litigation.[180] The Supreme Court has confirmed that class action waivers in arbitrations provisions are enforceable.[181] Such arbitration provisions and waivers should be conspicuous both in the company's notice of its terms and conditions for service, and in the terms and conditions themselves.[182] For example, to maximize the likelihood of enforcement, they should be "easily accessible and displayed in a sufficiently large viewing window to provide the user an adequate opportunity to review the terms, thereby eliminating any doubts that a reasonable user would have noticed them" and they should include easily understandable, balanced provisions to avoid a finding of unconscionability.[183] Additionally, best practices would require users to affirmatively accept the contractual terms before proceeding to the next step in the transaction or service provided.[184]

CONCLUSION

Protection of consumer personal information is a major issue faced not only by Americans, but by consumers across the globe. Both the frequency and severity of data breaches in the modern day of technology and internet usage have consistently increased throughout the twentieth century, developing into what some consider to be a modern "data breach epidemic." Neither federal nor state regulations fully address this epidemic in a way that provides consumers and businesses with clarity regarding their respective rights and duties post-data breach.[185] After their personal information is exposed, consumers face uncertainty in seeking relief, and the current circuit split in this area makes the choice of where

179. *See* HARRIS, *supra* note 21, at 36.

180. *See* Buese, *supra* note 22.

181. *See* Buese, *supra* note 22; *see, e.g.*, DirecTV Inc. v. Imburgia, 136 S. Ct. 463 (2015); AT&T Mobility LLC v. Concepcion, 563 U.S. 333 (2011).

182. *See* Buese, *supra* note 22.

183. Buese, *supra* note 22.

184. *See* Buese, *supra* note 22.

185. *See* Jones, *supra* note 20, at 813.

to file a claim of paramount importance if the injury is based on the theory of an increased risk of future harm (such as the increased risk for identity theft). From the perspective of businesses in possession of consumer personal information, conflicting laws relating to compliance creates an unnecessary burden for large businesses that operate in multiple jurisdictions.

There have been some attempts at a federal standard, but none have ultimately succeeded. Though it seems unlikely under the current political climate, enacting a federal data breach notification and data protection statute would go a long way in solving many of the issues currently faced by consumers and businesses. Confronted with this intimidating and rapidly changing technological landscape, California's new sweeping privacy legislation, the CCPA (effective January 1, 2020), will impose a multitude of new, extremely demanding notice, disclosure, and consent requirements on an array of business entities that conduct operations or handle the personal information of California residents. The CCPA will likely cause a shift in the landscape of data privacy law not just in California, but across the entire United States.

The data breach epidemic is not going away anytime soon, so in the meantime consumers should take extra precautions when evaluating whether, and with whom, they share their personal information. Additionally, businesses that use, collect, or store consumer personal information should maximize their security controls in place to prevent or decrease the likelihood of a data breach, and should also incorporate the use of both class action waivers and mandatory arbitration provisions to mitigate the potential effects of post-data breach litigation.