UCSD UNDERGRADUATE LAW REVIEW

TRACY TRUONG

Data Breaches in an Age of Technology: An Evaluation of Article III Standing and Expectations of Privacy

ABSTRACT. This essay will discuss Article III standing in regard to data breaches and expectations of privacy. The topic of standing is introduced in context with precedent court cases *Clapper v. Amnesty International* and *Spokeo, Inc v. Robins*, which highlight the limits of legitimacy of injury. These cases are then compared and contrasted to other decisions in recent circuit splits, showing that there is a lot of gray area on the type of injury sustained in a data breach. This article then looks at the current state of privacy domestically, coming to the conclusion that the U.S. needs a stronger national policy for privacy regulation to protect the consumer. Finally, such legislation is discussed, along with proposed solutions that consider the pros and cons of these discussions.

AUTHOR. Tracy Truong is a rising third-year student at UCSD majoring in Computer Science and minoring in Literature/Writing. She thanks her editor, Rishabh Raj, for his meticulous edits and constructive feedback.

INTRODUCTION

While data breaches are not a new phenomenon, the growth in technology in the last century has given people more reasons to fear the unethical exposure of their confidential information. Many states in the United States have differing laws on how to handle the aftermath of data breaches, but the discrepancies between these laws prevent the creation of a uniform standard on data privacy. There is currently no national law regarding the consequences of data breaches, and the reluctance of corporations to abide by certain regulations offers little stability for individuals who rightfully wish to protect their privacy. In the case that individuals find that their data has been exposed in a data breach, they can take legal action and have their concerns be represented in court. The ability to sue, however, leads to the debate over whether such individuals have standing under the Constitution, which is described in the Case or Controversy Clause in Article III, Section II, Clause I. This can be noted in numerous cases regarding data privacy and data breaches.

Under Article III, there are three conditions that plaintiffs must demonstrate to have standing: 1) they have suffered actual injury, 2) the injury can be traced to the defendant, and 3) the injury is likely to be redressed by a favorable decision.[1] The first condition, while simple in concept, is the chief source of conflicting rulings among courts on whether individuals have standing in data breach cases. A data breach occurs when "[T]here is a loss or theft of, or other unauthorized access to, other than an unauthorized access incidental to the scope of employment, data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data."[2] The first condition of standing typically only requires presenting proof of injury if a plaintiff suffers specific damage, such as the theft of material possession(s). However, theft of data in the digital age is less straightforward because often, the plaintiff does not know much more about their situation other than the fact that some data of theirs may have been stolen, which might or might not be detrimental for them in the future.

This describes the beginnings of the future harm principle. Despite precedents that deal with the same subject matter, there is no clear roadmap for what courts should do

---

1 *Substantial Interest: Standing*, Justia Law, https://law.justia.com/constitution/us/article-3/20-substantial-interest-standing.html#:~:text=%E2%80%94Although%20the%20Court%20has%20been,can%20fairly%20be%20traced%20to (last accessed June 25, 2022).

2 *38 CFR § 75.113 - Data Breach*, Legal Info. Inst., https://www.law.cornell.edu/cfr/text/38/75.113 (last accessed June 25, 2022).

here. The question of whether future harm should count for the first criteria for standing has brought about different interpretations, as it is difficult to prove that an individual's leaked information has been or will be misused.

Clapper v. Amnesty International USA (2013) introduced the notion of future harm in Article III Standing. In this case, numerous petitioners—consisting of journalists, attorneys, and human rights organizations—challenged former Director of National Intelligence, James Clapper, for authorizing government surveillance on non-U.S. citizens contacting U.S. citizens. They argued that the amendment to the Foreign Intelligence Surveillance Act (FISA), which allowed Clapper to surveil them, violated their First and Fourth Amendments rights by infringing on the right against unreasonable searches.[3] The plaintiffs claimed that their injury was both the violation of privacy and additional costs in seeking more confidential methods when communicating internationally. However, the case was dismissed in a 5-4 majority opinion. Justice Alito denied standing for the petitioners because "by inflicting harm on themselves based on their fears of hypothetical future harm," they did not display an injury that was "certainly impending."[4] Rather, their claims of harm were manufactured by fear, and fear does not equate to solid evidence. Though this case established that concrete proof must be provided to prove the legitimacy of injury, it is also important to consider Justice Breyer's dissent in *Clapper*, where he stated that the petitioners had standing because it was highly likely that their international communications would be intercepted, as they were continuously being monitored.[5] Thus the controversy that *Clapper* introduced was whether or not certain types of evidence presented in court could actually prove impending injury.[6] In the circuit split cases explored in Section 3, this article will examine and determine the applicability of *Clapper*'s decision against recent cases of data breaches.

Whereas *Clapper* introduced a general standard of what is required for standing, the details of what constituted injury-of-fact were explored in the 2016 Supreme Court case *Spokeo, Inc. v. Robins*. In this case, Thomas Robins attempted to sue Spokeo, a website that supplies data about individuals via a people search engine from online and offline sources, for publishing false information about him on the site as he claimed that it violated the Fair Credit Reporting Act's (FCRA) policy to "follow reasonable

---

3 Clapper v. Amnesty Int'l USA, 568 U. S. 398 (2013).

4 *Id.*

5 *Id.*

6 *Id.*

procedures to assure maximum possible accuracy of" consumer reports.[7] In his opinion, the false information published by Spokeo damaged Robins' image. But despite this, the Court ruled that Robins did not have standing because his concerns didn't stem from "actual or imminent" harm. Robins stated that Spokeo's false claim that he was wealthy would hurt his future employment prospects, but the court denied him standing, as his injury-of-fact was not "concrete and particularized."[8] Even so, the Court remanded the case to the Ninth Circuit Court, where they unanimously ruled that Robins did display sufficient proof of injury under the FCRA with a private right of action.[9] Instead of approaching the case directly with the aspect of future harm, Robins had the chance to argue that the misinformation about him on Spokeo violated his statutory rights, and "[t]he statutory right at issue protects against individual, rather than collective, harm."[10] This opened conversation about whether or not a violation of a private right of action was sufficient to prove injury for data breach cases. The Ninth Circuit decided that because statutory rights defend an individual, and because the harm inflicted on Robins was individualized and not collective, Robins had standing.[11] This line of reasoning did not require *Clapper* to be considered in this case as the Court avoided the idea of future harm.

These two cases attempted to place restrictions on what constitutes enough harm under the first criteria of Article III Standing. However, the line here is blurry because there is still no solid method of determining whether a plaintiff's harm is merely speculative or legitimate. While Robins was the only person harmed in his case and could seek a private right of action, data breaches leak sensitive information at a larger scale and can affect many more people. The Supreme Court did not think that Robins' accusations were sufficient enough for standing because his injuries were intangible, and therefore difficult to measure. While Robins was a lone individual who experienced something personal, those who suffer from a data breach harbor a collective fear. Data breaches can result in numerous severe consequences for consumers, as stolen credit card numbers, stolen emails, or exposure of social security numbers can lead to identity theft. This harm, if given tangible proof, would likely qualify for injury in standing. However, without tangible proof, it is significantly harder to gain standing, even though the fear of future harm is legitimate.

---

7 Federal Credit Reporting Act, 15 U. S. C. §1681e(b).

8 Spokeo, Inc. v. Robins, 578 U. S. 330 (2016)

9 *Spokeo, Inc. v. Robins*, Harv. L. Rev. (2016), https://harvardlawreview.org/2016/11/spokeo-inc-v-robins/.

10 *Id.*

11 *Id.*

Furthermore, with technological advancements, data has become much "bigger," meaning that companies control larger amounts of it.[12] It also means that industries have expanded the ways in which they can use and analyze consumer data, but they still struggle with organizing such a large capacity of data. This opens the door for more dangerous practices aside from data breaches that consumers might be unaware of. Also, since data is not property, sharing it becomes an agreement unbound by any current law.[13] Therefore, stolen data can only be proven through direct violations of general data breach guidelines. This makes it very difficult for plaintiffs to argue that they have been harmed because current data breach laws are not strong enough to provide "proof" to consumers. Corporations benefit from this arrangement because they only have to disclose how they use and share consumer data if a breach is significant enough to warrant an investigation. Thus, current laws surrounding data privacy in regard to data breaches are highly biased, and unjustly so. In an increasingly technological world and in light of a collectively heightened apprehension of the strength and ethics of internet and data privacy, the conditions that comprise the first criteria of Article III Standing should consider future harm and attempts at prevention of future harm as factors in an analysis of injury-of-fact legitimacy.

A new test for Article III Standing that identifies cases that favor the party whose data has been leaked would best implement this idea. Part 3 of this article discusses several circuit court decisions that suggest exceptions to the necessity of concrete evidence for proving injury. But because these decisions were made on a case-by-case basis, to create more certainty for future cases, a standard for data breach cases that should qualify for standing. Part 4 and Part 5 of this article discuss the current state of data privacy and conclude that there are laws that effectively hold companies accountable for leaking consumer information without consent but such laws do not currently exist nationally. Part 6 then concludes that preventative measures, such as having government organizations like the Federal Trade Commission (FTC), as well as private third-party companies, place restrictions on data usage in companies, should be

---

12 *What Is Big Data?*, Oracle, https://www.oracle.com/big-data/what-is-big-data/#:~:text=The%20definition%20of%20big%20data,especially%20from%20new%20data%20sources (last accessed June 25, 2022).

13 Cameron F. Kerry and John B. Morris, *Why Data Ownership Is the Wrong Approach to Protecting Privacy*, Brookings (June 26, 2019), https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/.

implemented to keep a tighter leash on the malpractice that is often detected in data breach cases.

I. ARTICLE III STANDING: CIRCUIT SPLITS

While *Clapper v. Amnesty International USA* and *Spokeo, Inc. v. Robins* denied the aspect of future risk in consideration of Article III Standing, recent circuit split decisions imply a lack of certainty surrounding the topic.

Before *Clapper*, a 2010 case called *Krottner v. Starbucks Corp.* established that the risk of identity theft was a viable reason for impending risk or harm. It followed a case at a Starbucks location where a laptop "contain[ing] the unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees" was stolen.[14] The plaintiffs—Laura Krottner, Ishaya Shamasa, and Joseph Lalli—were Starbucks employees who had their information in the stolen laptop, and appealed their case after the district court dismissed their claims that "Starbucks acted negligently and breached an implied contract under Washington law."[15] The Circuit Court, however, decided that although no proof was provided that whatever information found on the laptop was misused, the plaintiff qualified for standing because there was a risk of identity theft. It was easy for the Court to side with the plaintiffs' privacy concerns because the stolen laptop acted as a tangible representation of the stolen data. The theft itself implied the intention and high possibility of exploiting data.

Even with the decision in *Clapper* a few years later, the 2018 case *Stevens v. Zappos* reinforced that the risk of identity theft posed a big enough risk for standing, despite a lack of concrete evidence. *Zappos*, therefore, had similar lines of reasoning as *Krottner*. In this case, Theresa Stevens filed suit against Zappos.com, an online retailer, when her account on the site got hacked. Many other Zappos users also experienced a similar situation and claimed that the risk of identity theft from the hack was enough for proof of injury. After the breach, when Zappos advised users to change their passwords on other sites or programs if they utilized the same password on Zappos.com, they indirectly confirmed the risk of injury. This also confirmed that the nature of the stolen data could place consumers at risk, opening the possibility of identity theft crimes such

---

[14] Hanley Chew and Tyler Newby, *Appellate Court Finds Risk of Identity Theft Sufficient to Establish Standing, Circuit Split Worsens*, JD Supra, https://www.jdsupra.com/post/contentViewerEmbed.aspx?fid=103ed29e-81b0-494b-bebe-61019a920be4 (last accessed June 25, 2022).

[15] Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).

as "pharming"[16] or "phishing."[17] While the Supreme Court denied this case certiorari, the Ninth Circuit agreed with the Sixth, Seventh and D.C. Circuits that "in an analogous context" to *Krottner v. Starbucks Corp.*, the plaintiff's fear of future harm "sufficiently alleged standing based on the risk of identity theft."[18] This offered a loophole around the holding in Clapper, acknowledging that proof of injury could be extracted from the context of a scenario not necessarily provided by the plaintiff; Zappos's actions following the breach showed that the plaintiffs faced some sort of risk. While this benefited Stevens' argument for her case, it also shows how in the event of a breach, companies are the most aware of what happens to the leaked data. Despite this, under the current doctrine of Article III standing, consumers are expected to show proof for their injury when they are somewhat blind to what is happening. Under this current system, consumers arguably don't have any reason to believe they have been harmed, and therefore don't have standing, if they don't know what has happened to their data. However, this is synonymous to saying that if companies don't disclose any malpractice, then they have not done anything harmful. But this is not true in many data breach cases, and thus, the current doctrine of standing heavily favors companies in data breach cases.

As opposed to these Circuit Court cases that sided with the plaintiff, recently, *Tsao v. Captiva MVP Restaurant Partners* (2021) rejected the idea of future harm. In this case, a restaurant chain, PDQ, suffered a data breach and admitted hackers "may have . . . accessed" credit cardholder names and accounts.[19] Tsao, a PDQ customer, argued that he and other customers had "been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud."[20] Tsao's fear drove him to "voluntarily [restrict] access to his preferred payment cards.[21] And by canceling his cards, he voluntarily spent time safeguarding his accounts."[22] The

---

16 Pharming entails the act of "directing internet users to a bogus website that mimics the appearance of a legitimate one, in order to obtain personal information such as passwords, account numbers, etc." Pharming, New Oxford American Dictionary (3rd ed. 2010).

17 Phishing involves "the creation of false digital resources intended to resemble those of legitimate business entities, such as a website or email" to invoke fraud. *Phishing*, Legal Information Institute, https://www.law.cornell.edu/wex/phishing#:~:text=Phishing%20is%20a%20type%20of,via%20email%20or%20URL%20to (last accessed June 27, 2022).

18 Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).

19 Tsao v. Captiva MVP Restaurant Partners, *LLC*, 986 F.3d 1332 (11th Cir. 2021).

20 *Id.*

21 *Id.*

22 *Id.*

Eleventh Circuit felt that because there was no immediate or targeted threat, Tsao's claims and actions were based upon "a nonparanoid fear."[23] The Eighth Circuit additionally reasoned that since a Government Accountability Office (GAO) report claimed that credit card information alone is not enough to raise the risk of identity theft, Tsao's claims of imminent harm were faulty.[24] While the GAO states that "unauthorized use of a stolen credit card number" is a component of identity theft, "compromised credit or debit card information, without additional personal information" cannot damage an individual without additional information.[25] Ultimately, "because he [couldn't] demonstrate that there is a substantial risk of future identity theft—or that identity theft [was] certainly impending—and because he [couldn't] manufacture standing by incurring costs in anticipation of non-imminent harm," Tsao did not have standing.[26]

Contrasting *Krottner*, and later *Zappos*, with *Tsao*, it can be concluded that in a data breach, risk of identity theft, even with no solid proof, may be enough for standing. This means that what *Clapper* determined was not definitive; rather, it provided a gray area where different cases could yield different results. With the context of the cases following *Clapper*, injury by future harm can be defined by whether or not certain leaked information is substantial enough to cause immediate harm. In *Krottner* and *Zappos*, the risk of identity theft was considered to be significantly high due to the nature of the data that was released. Though Tsao reasonably believed that he could be at risk of fraud or financial ruin given the exposure of his credit card information, there were precautions that could have greatly lessened the risk. These cases seem to draw a line between what constitutes imminent harm and what doesn't, but they still do not address the actual issue of future harm in regard to standing. For Tsao's case, though credit card information alone does not lead directly to identity theft, there is also no telling how hard the hackers will pursue the information they stole. Because the courts dismissed Tsao's case, not agreeing to his claims of harm, it gives reason for companies to believe that there are no consequences if information that is not associated with a direct indication of identity theft is stolen by hackers. Another question that Tsao's case raises is which party is responsible for mitigating the harm done in a data breach. Because they denied him standing, Tsao had the responsibility to ensure that his data would not be misused. If they granted him standing, then the PDQ restaurant chain

[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.*

would have had this responsibility. Thus, the issue of standing extends further than solely determining whether or not plaintiffs suffered harm from a data breach. The lack of a mechanism to hold companies accountable for breaches puts consumers at a dangerous disadvantage.

According to the Federal Trade Commission, identity theft is possible when someone obtains information regarding an individual's address, bank information, medical insurance, account numbers, or Social Security number.[27] For someone to know if their identity is stolen, they would need to proactively monitor their bills and bank account statements to detect fraudulent activity. Even if Tsao had standing, he would still have to do this, as he does not know whether his stolen information is being used for fraud. However, because the court concluded that his claims of harm were not imminent, they discredited the possibility that he was susceptible to identity theft and sided with the PDQ restaurant business over the consumer. Additionally, the Eleventh Circuit, along with other courts with similar opinions, did not explore the scenario of what would happen in the future if Tsao found out that all along, hackers did indeed use his information and engaged in identity theft. The court's opinion, then, would be inconsistent because they didn't consider the fact of future harm as heavily as in the *Krottner* or *Zappos* cases upon seeing Tsao's lack of evidence. Conversely, if the court granted Tsao standing, and Tsao in the future finds that his information was not misused, then the court would have stronger reason to believe that future harm should not qualify for Article III standing. This uncertainty is one that is yet to be explored further. While one option to resolve this would be to curate a test to more accurately define "imminent harm," another option is to approach the issue from a different standpoint where the consumer does not have to struggle to prove their case. A major factor missing from these cases is an emphasis on the responsibility companies have in protecting their consumers' information. Data breaches would occur far less often if companies enacted reasonable security measures. Instead of placing the burden on the consumer to monitor the status of their security, the standard should be for companies to follow stricter security guidelines. These guidelines must come in the form of rules, not merely recommendations from organizations or agencies such as the FTC.

Because Article III Standing is vague in its criteria, it still makes sense to consider the correlation and attachment of future harm to an analysis of injury-of-fact. Additionally, since *Clapper*, technology has grown so rapidly that the conclusions made in the case are outdated. Stronger regulations to ensure fairness in privacy should

---

[27] Amy Hebert, *What to Know about Identity Theft*, Consumer Advice (2022), https://consumer.ftc.gov/articles/what-know-about-identity-theft.

be considered in light of the significant damage data breaches cause. Along with this, consumers who have been harmed by companies with data breaches should be able to sue and hold companies accountable for their mistakes. This will force companies to value data privacy and take FTC guidelines on data privacy more seriously.

II. CURRENT STATE OF DATA PRIVACY

Because there are no federal data privacy laws, there is no national standard for privacy expectations. Because of the relationship between data breaches and privacy, current data privacy laws should be examined to establish a correlation to standing and legitimacy of injury.

A good model for rigorous privacy policy is the European Union's General Data Protection Regulation (GDPR) of 2018. Replacing its predecessor, the Data Protection Directive, the GDPR's primary goal was to more strongly protect consumers against companies who use their personal data in light of the past decades' worth of technological advancements. The GDPR emphasized accountability and consent, explicitly stating guidelines that companies must follow when processing consumer data. These rules are outlined in seven detailed principles, which thoroughly create a standard for privacy expectations and limit the freedom that companies have in dealing with consumer data internally.[28] It assumes a privacy-by-default situation for consumer and company relationships. The GDPR is comparable in this attitude towards privacy to the California Consumer Privacy Act (CCPA), also put into effect in 2018.

A. Analysis of the CCPA

Before the CCPA, California legislation that dealt with data breaches mainly consisted of one law, the California Data Breach Notification Law, which required any company "that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system" to California residents.[29] This applied only to unencrypted data or encrypted data that had been leaked with the encryption key because encrypted data on its own is nearly impossible to access without an encryption key.

---

[28] Christian Wigand, Guillaume Mercer, and Katarzyna Kolanko, *Press Corner*, European Comm'n (2020), https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166.

[29] CA Code CIV. § 1798.82 (2011)

It was because of this law that the 2017 Equifax data breach was brought to light, as it reportedly "affected consumers [totalling] to over 147 million U.S. consumers, approximately 15.8 million of whom were California residents. Social Security numbers, birth dates and addresses had been compromised, as well as in some instances, driver's license numbers, credit card numbers; and credit dispute documents."[30] The breach stemmed from an overlooked and ignored, but easily preventable, vulnerability in the corporation's network and ultimately cost Equifax a $575 million dollar settlement to the FTC and other agencies involved in the breach.[31] Had the CCPA been enacted during this time, however, Equifax would have been much more compromised. Since Equifax is an important credit reporting company, the breach settlement would have been even more costly, somewhere in the billions, which would have likely terminated the company. While the prospect of Equifax terminating would not undo the damages of the data breach, it sets a clear standard for privacy. The strengthening of data security laws, therefore, are for the benefit of citizens.

It was also because of the California Data Breach Notification Law that Uber Technologies was caught and severely reprimanded by the public for trying to cover up their hack and data breach in 2016. They "revealed that [the company] acquiesced to the hacker's demands by paying the $100,000 ransom and then engaged in a plan to cover-up the hack for more than a year wherein Uber's customers and drivers were never informed that their personal information had been stolen."[32] Uber's attempted cover-up reveals just one of the many unethical practices that companies may engage in to avoid public backlash from a data breach. Companies would rather protect themselves instead of their workers and consumers because admitting fault could severely damage their reputation. Companies who fear this, yet continue to refuse transparency, show how easily they take advantage of the lack of national privacy laws to continue and even normalize their unethical practices of using, analyzing, or even

---

30 *145 million Social Security Numbers, 99 million addresses and more: Every type of Personal Data Equifax lost to hackers, by the numbers*, The Washington Post, https://www.washingtonpost.com/news/the-switch/wp/2018/05/08/every-type-of-personal-data-equifax-lost-to-hackers-by-the-numbers/ (last visited June 4, 2022).

31 Jacqueline Connor and Tiffany George, *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, Fed. Trade Comm'n (Sept. 18, 2021), https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach.

32 *Cyber Security: When the Cover up Is Worse than the Crime: Uber & the Consequences of Hiding a Data Breach*, Poole & Shaffery LLP, https://www.pooleshaffery.com/news/2017/december/cyber-security-when-the-cover-up-is-worse-than-t/ (last accessed June 25, 2022).

selling consumer data behind their backs. After they were caught, Uber agreed to increase their security measures and provide quarterly security updates to the states for the next two years.[33] Though this was part of Uber's plan to move forward and learn from their mistakes, it also seemed like a way for them to earn back trust from those who were harmed by the breach. While it was unlikely that they would have another breach in the same manner, it also did not guarantee that Uber wouldn't engage in other unethical practices in the future. Though there is no evidence that the preventative measures that Uber took following the breach were or were not effective, after the breach was brought to light, Uber's former chief security officer Joe Sullivan still attempted to push the narrative that the incident was not a coverup. Rather, he stated that the breach came from Uber using their bug bounty program[34] to identify security weaknesses.[35] Uber fired Sullivan for his poor handling of the breach, but his defense of Uber's unethical security practices shows that without stricter privacy guidelines for data breaches, companies can freely interpret what they believe what proper security should look like. While the CCPA provided strict enforcement on data breaches, on the issue of privacy itself, enforcement is inadequate. Mary Stone Ross, a co-author of the initiative for the CCPA, states that "in the legislative compromise [of the CCPA], only the attorney general can enforce the CCPA (except for data breaches). Unfortunately, the California attorney general's office predicts that even with additional resources, they will only be able to bring three enforcement actions a year, rendering the CCPA largely toothless."[36] Although the CCPA does handle data

---

33 Bill Chappell, *Uber Pays $148 Million over Yearlong Cover-up of Data Breach*, NPR (Sept. 27, 2018), https://www.npr.org/2018/09/27/652119109/uber-pays-148-million-over-year-long-cover-up-of-data-breach.

34 A bug bounty "is a supporting function to an existing Vulnerability Disclosure Program (VDP) [that] encourages the reporting and disclosure of security vulnerabilities found in software and/or infrastructure by incentivizing vulnerability reporters with rewards or compensation." Deana Shick, *Chapter 1: What is a Bug Bounty Program?,* Bug Bounty COI (May 4, 2021), https://bugbountycoi.org/2021/05/04/chapter-1-what-is-a-bug-bounty-program/#:~:text=Simply%2C%20a%20Bug%20Bounty%20program,reporters%20with%20rewards%20or%20compensation.

35 Tom McClelland and Austin Mooney, *Uber Criminal Complaint Raises the Stakes for Breach Response*, JD Supra (Sept. 1, 2020), https://www.jdsupra.com/legalnews/uber-criminal-complaint-raises-the-98984/.

36 Katharine Schwab, *I Helped Draft California's New Privacy Law. Here's Why It Doesn't Go Far Enough*, Fast Company (Dec. 30, 2019), https://www.fastcompany.com/90444501/i-helped-draft-californias-new-privacy-law-heres-why-it-doesnt-go-far-enough.

breaches effectively, without adequate enforcement, companies will continue to engage in unethical practices because they will likely avoid severe consequences.

The outcomes of the Equifax and Uber data breaches proved the effectiveness of existing data privacy laws, but also raised the question of what would happen if the notification law didn't exist. Likely, these companies would have gotten away with malpractice, putting consumers at risk. This reinforces the conclusion found in the previous section, where it was found that emerging privacy laws must hold corporations accountable in some standard way.

These conclusions might suggest that data could be thought of as property. If so, cover-ups such as the one done by Uber could be considered as valid evidence for concrete theft. However, if data could be owned and sold, it then follows that all types of data, including individual data, would have a price. But this is not reasonable, as data should not be considered a "commodity."[37] It is simply impractical to commodify data, as the only way to preserve data is for it to be shared. While data can be sold or shared by companies (such as through consumer information they receive via their online cookies), consumers are not selling this data themselves. With an opt-in policy (usually a 'sell my information' or 'do not sell my information' toggle), selling data is analogous to participating in a survey. Privacy can be considered a right, but personal data cannot. Thus, if data should not be considered as property, but rather, as entailing the act of sharing information, then consumers still cannot reliably gauge how and for what corporations use their data. These concerns were reflected in the creation of the CCPA, which took an effective step forward in the strengthening of privacy protections by setting clearer limits on what can and cannot be done with data and by giving consumers the transparency they should have.

B. Private Right of Action in the CCPA

One of the most crucial aspects of the CCPA that is not in the GDPR is its inclusion of an explicit but limited private right of action, which allows private plaintiffs to sue companies directly in the event of a data breach. If a consumer proves that a company leaked their "nonencrypted and nonredacted personal information"

---

[37] Cameron F. Kerry and John B. Morris, *Why Data Ownership Is the Wrong Approach to Protecting Privacy*, Brookings (June 26, 2019), https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/.

the consumer has the right to press charges for statutory damages.[38] This sets a minimum standard of security for companies to enact, with penalties if the company does not comply. The existence of this private right of action therefore places a bigger responsibility on the government to ensure that consumer data is protected by enacting "reasonable security measures."[39] Not only does this provide more detailed regulations that hold corporations accountable, it also gives consumers more outlets to bring cases to court. In fact, "[I]n 2021, 281 federal court cases were filed in, or removed to, federal court and referenced either the 'CCPA' or the 'California Consumer Privacy Act,'" which "represents a 44.10% increase in litigation filings." This implies that since the CCPA went into effect, CCPA class action lawsuits have highly increased in numbers.[40]

However, even if statutory damage is proven under a CCPA claim, standing to sue needs to be evaluated separately. The case *Arifur Rahman v. Marriott International, Inc.* (2021) demonstrated this. In this case, the plaintiff, Arifur Rahman, wanted to sue a franchise in Russia for the Maryland-based Marriott International hospitality company for a cybersecurity breach that violated the CCPA. In this breach, "names, addresses, phone numbers, email addresses, genders, birth dates, and loyalty account numbers without authorization" were leaked. However, the U.S. District Court dismissed the case because "sensitive information" was not leaked, and therefore did not fulfill the requirements for the right to sue. The outcome of this case is similar to many other ones regarding data breaches.[41] Plaintiffs often have to rely on common law causes of action to prove substantial risk or imminent harm.

The holding in *Rahman* was therefore similar to *Tsao*, where the Court also denied standing due to the supposed lack of sensitive information exposed during PDQ's breach. These cases, then, seem to conclude that breaches which do not create apparent risk of identity theft will not be as rigorously considered in court. While certain types of data are more sensitive than others, it would be wrong to say that one type of data is more valuable than the other. This raises the question of whether it is fair to decide harm based on the type of information leaked in a breach. With technology continually advancing, different types of complex data are arising, which implicates other practical

---

38 CA Code CIV. § 1798.82 (2011)

39 CA Code CIV. § 1798.82 (2011)

40 Jena M Valdetero and David A Zetoony, *CCPA Litigation up 44.1%*, The Nat'l L. Rev. (Mar. 7, 2022), https://www.natlawreview.com/article/ccpa-litigation-441#:~:text=The%20California%20Consumer%20Privacy%20Act,institute%20reasonable%20and%20appropriate%20security.

41

concerns regarding privacy and security, outside of just identity theft. By denying plaintiffs standing because their leaked information was not sensitive enough, recent court cases set a dangerous precedent for the future by dismissing violations of privacy, when they can be just as harmful as data breaches.

C. Third Parties and Improving Data Privacy Law

Both the GDPR and the CCPA value transparency between companies and consumers. While the GDPR requires citizens' consent prior to any sort of data processing,[42] the CCPA has an opt-out policy,[43] allowing companies to access data by default unless otherwise chosen by the consumer.

The CCPA overall provides more freedom to consumers regarding their data, such as the right to know how their data is collected, used or shared, the right to delete the data they have shared, and the right to opt-out on the sale of their data.[44] Although this is limited to just California and not the rest of the nation, it marks the beginning of progress in protecting consumer data and standardizing expectations of privacy. It also calls into question whether precedent policies should change to reflect these expectations given the emerging importance of technology.

The United States has historically expected individuals to be responsible over their data, rather than having companies abide by certain data restrictions. This concept can be seen through the third party doctrine in cases such as *United States v. Miller* and *Carpenter v. United States*. But looking at these cases, it is clear that the opposite should be true: companies should enact privacy policies to protect consumer data because the culture of data sharing has changed significantly.

In 1976, the Supreme Court case *United States v. Miller* established the third party doctrine, which states individuals do not have a "reasonable expectation of privacy" over information they give to a third-party data collector.[45] In this case, Mitch Miller was accused of leasing an undocumented whiskey distillery, which the sheriffs of

---

42 *The EU General Data Protection Regulation*, The EU Gen. Data Prot. Regulation, https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#R32 (last accessed June 26, 2022).

43 Rob Bonta, *CCPA Opt-out Icon*, State of California - Dep't of Justice - Office of the Attorney General (Mar. 16, 2021), https://oag.ca.gov/privacy/ccpa/icons-download#:~:text=The%20California%20Consumer%20Privacy%20Act,stop%20selling%20their%20personal%20information.

44 *Id.*

45 United States v. Miller, 425 U. S. 435 (1976).

Housten County, Georgia proved through acquiring Miller's bank transactions.[46] While Miller claimed that this seizure of bank transactions violated his Fourth Amendment right to privacy, the Court held that since banks are third parties, the sheriffs could legally obtain Miller's information because he no longer had a "reasonable expectation of privacy" with those documents.[47]

However, in 2018, *Carpenter v. United States* made an exception to this doctrine. This case follows Timothy Carpenter, who was charged for involvement in a robbery. Even though Carpenter was not one of the four people originally targeted as suspects, transactional records of cell phone service of the four suspects traced the police back to him.[48] The Court held that although the records of cell phone service were in the hands of a third party, Carpenter still had a reasonable expectation of privacy with that information and seizing it violated his Fourth Amendment rights, *Carpenter* was a landmark decision for holding that exploiting location data was a violation of privacy, even though it was retrieved through third-party data collectors, because it acknowledged the shift in technology in regard to precedent.

While *Miller* dealt with third-party information in regard to bank records, holding that they were not protected under the Fourth Amendment, *Carpenter* dealt with location data. When *Miller* was decided, data was thought of as tangible, as information in *Miller* was in the form of paperwork and technology had relatively weak capabilities during the time. It was therefore logical to conclude that since Miller willingly gave the bank his paperwork he had no reasonable expectation of privacy with that information. However, years later, *Carpenter* held that GPS location tracking was forbidden, despite the third party doctrine, because GPS location tracking data is not tangible. Only technology can be capable of collecting such data. After her concurrence in *U.S. v. Jones*, another case regarding third-party data, Justice Sotomayor stated that "[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[49]

---

46 *Id.*

47 *Id.*

48 Carpenter v. United States, 585 U. S. ___ (2018).

49 John Villasenor, *What You Need to Know about the Third-Party Doctrine*, The Atlantic (Dec. 30, 2013), https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/.

This evolution in ideology must also happen with data breaches and standing. While the current agreement—that an individual is denied standing if they cannot prove imminent harm—may have been suitable for a time of simple data (as is evident in *United States v. Miller*), today's technological capabilities have made certain types of data more complex through additional processing. This issue extends beyond mere paperwork, and can bring imminent harm in the case of data breaches. Data collected on a large scale and analyzed through complex computer algorithms, is described today as "Big Data." Additionally, given the increase in sensitive data since the age of the Internet, it is unreasonable to expect the average person to not have expectations of privacy about their data. Many everyday tasks now rely on non-physical forms of data, making it infeasible for people to constantly keep track of all of their data. In light of the increasing amount of personal risk in data breaches, Courts should no longer deny fear as a factor in the Article III standing criteria.

III. STRENGTHENING PRIVACY LAWS

In many cases, individuals who give their information do so without realizing exactly what they are doing — for instance, agreeing to terms and conditions before using an application. Most information used to be transferred tangibly, such as through paperwork (as was the case in *United States v. Miller*), but today, information is mainly transmitted through technology and the internet. Data sharing has transitioned from being voluntary to being a routine necessity. To reflect this change, and prevent companies from exploiting citizens' privacy, new policies akin to the GDPR and CCPA must be enacted to strengthen regulation on the types of data that companies can collect and increase transparency about what types of data they collect. Just as the lack of concreteness in future harm exists in the criteria of Article III Standing, there is a lack of regulation in how companies can use consumer data, and both discrepancies harm consumers more than companies.

This was seen in the 2018 Cambridge Analytica-Facebook Scandal, where "Facebook allowed a third-party developer to engineer an application for the sole purpose of gathering data. And the developer was able to exploit a loophole to gather information on not only people who used the app but all their friends—without them

knowing."[50] This data ended up in the hands of Cambridge Analytica, a political consulting firm working with the Trump campaign. This incident highlights the conflicting interests that companies have in protecting consumer data. Because a lot of technology companies' profits come from their software based on user data analysis, it is difficult for them to bar themselves from having access to such data, despite the privacy interests of users. Thus, this scandal exposed Facebook's preference of profit over user privacy, evidenced by their lack of policies for protecting users. The impact of this scandal reaches far beyond the reputation of Facebook and Cambridge Analytica, because it brings to light issues of companies finding loopholes in the law to use and exploit consumers' data. Facebook faced many lawsuits following coverage of the scandal. D.C. attorney general Karl Rancine filed one of the biggest lawsuits regarding the scandal in the United States. Allegations were made that Facebook was aware that Cambridge Analytica was using user data, and therefore misled more than 87 million users.[51] In cases like this, consumers and companies are placed at unequal footing, with companies almost always having the upper hand. While standing wasn't the central issue in this case due to how large-scale it was (Racine sued Facebook for violating the District's Consumer Protection Procedures Act, D.C. Code §§ 28-3901, et seq. ("CPPA"),[52] the same principle applies that consumers are highly disadvantaged in data breach cases.

This event also brings to light the question of what "imminent harm" can mean in terms of data collection. In this case, consumer data was used to manipulate the types of posts and advertisements users saw on Facebook, which heavily affected votes in the 2016 United States election.[53] While consumers weren't harmed in the sense of personal injury, their information was exploited nonetheless. Consumer information

---

50 Alvin Chang, *The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram*, Vox (Mar. 23, 2018), https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

51 Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout so Far*, The New York Times (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

52 *145 million Social Security Numbers, 99 million addresses and more: Every type of Personal Data Equifax lost to hackers, by the numbers*, The Washington Post, https://www.washingtonpost.com/news/the-switch/wp/2018/05/08/every-type-of-personal-data-equifax-lost-to-hackers-by-the-numbers/ (last visited June 4, 2022).

53 Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout so Far*, The New York Times (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

can also be leaked by Big Data practices, as they have the ability to use consumers' current data to predict future data, thus taking away some freedoms in the way companies can change their policies according to such data. Data cannot be contained as easily as property. Once given or shared, data cannot be given back because information cannot be owned. Though people can have ownership and privacy rights for data located in a database, most data transmitted through the internet is not protected. Formal violations don't exist in most cases, as there are no federal laws for privacy. Thus, it is unfair that courts get to decide whether somebody else's injury is significant enough for standing. Furthermore, what is not deemed imminent harm today might not necessarily be true in the future. Therefore, there should be a federal standard, similar to the CCPA, to reflect the growing prominence of data breaches and their damaging effects.

A. Current Discussions

In a Commerce, Science and Transportation Committee Senate hearing on federal data privacy legislation, commissioner and acting chairman of the Federal Trade Commission (FTC) Maureen Ohlhausen stated that "[A] federal privacy law needs to be a strong one. Federal privacy legislation should support robust enforcement by the FTC, allowing the agency to obtain meaningful results."[54] Strictly enforcing such privacy legislation would hold businesses accountable and also define a limit for how data can be handled. Given the GDPR's success in Europe, America should also implement its own national privacy law. Ohlhausen also suggests that "[T]he FTC needs to be able to fine companies for first time violations of the new [privacy] law and Congress must also provide the FTC with new resources." These specifications, along with the FTC's current policies regarding fair business practices, would set up a system of policing to prevent companies from abusing the use of consumer data. Furthermore, a new government agency that focuses specifically on helping consumers make the best decisions to protect the security of their data should be established. This, along with giving the FTC more power, would better prevent privacy violations and protect sensitive consumer data. This new agency could follow the structure and intentions of the Consumer Financial Protection Bureau (CFPB) which "is an independent bureau within the Federal Reserve System that empowers consumers with the information

[54] *Protecting Consumer Privacy, Hearing Before the S. Comm. on Commerce, Science and Transportation,* 117 Cong. 9 (2021) (statement of Maureen Ohlhausen, Former Acting Chair of the Federal Trade Commission).

they need to make financial decisions in the best interests of them and their families."[55] Their main goal is "fairness and transparency," which are characteristics pertinent in the realm of data protection.

In many data breach cases, companies have been found at fault for not properly protecting data that they are trusted to keep safe. Though Ohlhausen opposes a federal private right of action, former Attorney General of California and current Secretary of Health and Human Services Xavier Becerra believes that "[C]onsumers need the authority to pursue remedies themselves." If a federal law was introduced so that more consumers could have the ability to protect themselves, it would lead to an influx of investigation cases. Becerra says that a private right of action, like the one provided by the CCPA, would "complement and fortify the work of state enforcers." Additionally, it would validate the concerns that consumers have in a data breach, as they would have the right to sue companies directly. Thus, stronger privacy laws would act as "a federal privacy protection floor, not a ceiling."

B. Solutions in Context With Current Discussions

Despite the different arguments presented throughout different circuit split cases, the Second Circuit court clarified in *McMorris v. Carlos Lopez & Associates, LLC* (2021) that all courts have been open to the possibility of increased risk as sufficient justification for standing, but no cases have been strong enough to act on that possibility.[56] Therefore, while it is worth looking at the aforementioned contrasting circuit court decisions, there is a general consensus that increased risk generally does demonstrate harm.

In summary, there are three general scenarios for determining injury in data breach cases. The first is whether or not concrete evidence has been presented: this is demonstrated most clearly in *Krottner*, where the laptop was physical evidence of stolen data. The second is whether or not the nature of the leaked data is substantial enough for injury: this is seen most clearly in *Zappos*, where the type of data leaked by the retailer could easily lead to identity theft. The third is whether or not increased risk can imply injury. According to the Second Circuit in *McMorris*, this last situation is not out of the question, but there is yet to be a case to contradict the current policy that increased risk can be directly correlated to injury. The second and third scenarios

---

55 *The Federal Register*, Fed. Register :: Request Access, accessed June 26, 2022, https://www.federalregister.gov/agencies/consumer-financial-protection-bureau.

56 McMorris v. Carlos Lopez & Associates, LLC, 995 F.3d 295 (2d Cir. 2021).

present the most controversy, but could be resolved by a type of general test. Similar to the private right of action introduced in the CCPA, this test would consider whether or not the data leaked in a breach is unredacted or unencrypted. If so, it should be a factor heavily considered for heightened risk, substantial risk or injury, and thus, standing.

C. A Stronger Test for Standing

Testing the feasibility of this approach would concern court cases in which data is leaked from a corporation, regardless of the manner in which such data is leaked. In *Krottner*, the laptop's data was both unredacted and unencrypted. In *Zappos*, the specific type of data was not specified, but a database was breached, implying that sensitive and unprotected information was leaked. In *Tsao*, the credit card information leaked by the restaurant chain was likely unprotected as well. In these three cases, a lot of the disagreements regarding the qualifications for standing were rooted in whether or not the data leaked was harmful or not, but the approach suggested here places the focus on whether or not general types of data are likely to be misused or not. This allows injury to be more determined by the relationship between the corporation and the data they were meant to protect, as opposed to the consumer and the data they lost. Thus, in *Krottner*, this approach recognizes that the information on the laptop was not meant to be placed in such an accessible location, making Starbucks responsible. In *Zappos*, the data leaked was unprotected, making the Zappos company responsible. In *Tsao*, unlike how the case was actually decided, because the data leaked was unprotected, the PDQ restaurant chain should have been held responsible. These three cases show that whether or not data leaked in a breach is unprotected should determine whether or not corporations have done damage and should be held responsible. This approach does not alter the definition of standing, but it provides a standard for what is expected of corporations who place their consumers at risk. Although this test is admittedly ineffective for data breach cases that involve breaches of protected data, it is almost impossible to develop a comprehensive test that can be applied to data breach cases of all types. As previously mentioned, the concept of "Big Data" involves the constantly evolving process of storing and handling large amounts of data in complicated databases. Thus, standing for data breach cases must be evaluated in the context of a breach itself. This is what the approach presented in this section is meant for, as laws such as the CCPA have addressed breaches in the same context. While the

test is geared toward a small band of cases, it can still greatly help courts determine legitimacy of injury.

D. Government Action and Private Regulation

A wider approach to the problem of data breaches as a whole is to introduce laws for supporting private regulations, both within government sectors and organizations independent from the government (to reduce political conflict and bias). Like Maureen Ohlhausen suggested, giving more power to agencies such as the FTC to keep a leash on companies' data handling practices can lower the frequency of data breaches. As Uber's cover-up suggests, however, new laws alone may not be sufficient because companies will inevitably ignore or find a loophole around them. Instead, regular checks to ensure that companies ethically handle their consumers' data is more effective. Since this regulation is important, execution for the means to do so is also crucial. Recent developments with Artificial Intelligence can serve as a tool for advanced security measures, with some data analytic tools being created through machine learning practices to perform tasks like predicting cyber attacks through data processing. This area of analytics has yet to be perfected, especially since it becomes less efficient as data areas grow, but it is currently being developed. Along the same lines of data analysis is data provenance, which traces the actions throughout the lifespan of certain data, from its creation up until its current status. For example, data provenance can trace all activity of a file, including its creation date and where the data of the file is propagated to. By constantly running audits on data systems and data provenance, threats of data being misused can be easily detected. Verizon data breach reports[57] suggest that most data breaches occur due to human error and increases in ransomware attacks.[58] This shows that data breaches are often preventable and highlights the importance of taking steps for data protection. Through private policies, constant enforcement of cybersecurity practices would motivate companies to better protect consumer data and avoid negligent practices from causing data breaches in the future. Not only would this be financially beneficial, as data breaches are very expensive, it also perpetuates trust and comfort surrounding the expanding uses of technology.

---

[57] *2022 Data Breach Investigations Report*, Verizon Bus. (2022), https://www.verizon.com/business/resources/reports/dbir/.

[58] Ransomware is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. *What is Ransomware?*, Proofpoint (2022), https://www.proofpoint.com/us/threat-reference/ransomware (last visited June 28, 2022).

Companies continue to use technology to perform complicated analyses on data they collect from consumers, but regulation is still key in preventing companies from malpractices in their data collecting. Therefore, the combination of stricter privacy standards and regular checks using technology tools would hold companies accountable and prioritize consumer safety, lessening the errors that cause data breaches, such as not encrypting sensitive information.

Testing the feasibility of this suggestion can be done by applying it to previous data breaches from corporations. Because the approach is focused on prevention itself, it creates a standard for what is acceptable for how corporations store, access and protect consumer data and information. This suggestion can follow the structure of institutions that already have internal security protocols to protect the consumer, like banking companies who are required to have regulations such as secure infrastructure and authentication.[59] This follows the mindset of an "opt-out" policy, which defaults to privacy unless the consumer decides otherwise. Thus, while private regulations may not directly impact how injury of fact is determined in court, they can add protection not yet included in data breach laws such as the CCPA. In the Uber breach, Uber was required to generate security updates after the breach to prove that they were improving their security measures. While something like this is not necessarily enforced with this approach, generating regular reports is implied. Because the Equifax and the Uber breaches were caused by weaknesses in security systems, it is not enough for companies to reassure the public that they do internal checks, as there is no true way of verifying that these checks are effective. Thus, with the active role of private regulation by a third party not affiliated with a corporation, claims of effective security are likely to be reliable. Not only would this reduce the amount of data breaches that occur due to carelessness, it would also provide corporations credibility when handling consumer data.

CONCLUSION

Data breaches in today's digital age are growing increasingly common, yet there is little precedent for how to manage their aftermath. With the criteria listed for Article III Standing, it is difficult for citizens to successfully pursue legal action if their data or

[59] David Smith, *5 Ways in Which Banks Secure Their Data*, Endpoint Protector Blog (2022), https://www.endpointprotector.com/blog/ways-banks-secure-data/.

information has been leaked. *Clapper v. Amnesty International* was the most significant Supreme Court case to introduce the inability to use future harm to prove concrete harm. However, it is found in an analysis of recent circuit splits that this method of thinking is flawed because the risk of future identity theft is widely regarded as legitimate harm. Additionally, analysis of how laws and precedent cases regarding data privacy have changed to define a standard for what citizens should expect from corporations who collect their data reveals the need for a national standard for data privacy. Given the issues regarding standing and data privacy, solutions are proposed to benefit consumers. Mainly emphasized is the fact that a stricter leash needs to be placed on corporations so that consumers can feel more at ease when providing their personal information. Currently, the laws that exist are biased against consumers, and thus while stricter policies such as the CCPA are steps in the right direction, a lot more still needs to be done.