Volume 123 | Issue 1 Article 10

September 2020

The Threat of Data Misuse and an Injury-In-Fact: Establishing a Uniform Framework for Constitutional Standing in the Privacy Era

Isabella Anderson
West Virginia University College of Law

THE THREAT OF DATA MISUSE AS AN INJURY-IN-FACT: ESTABLISHING A UNIFORM FRAMEWORK FOR CONSTITUTIONAL STANDING IN THE PRIVACY ERA

I. INTRODUCTION

The last two decades have seen a rise in the use of technology to facilitate everything from maintaining personal finances, conducting everyday business, staying in touch with one's colleagues and family members, and more. In order to keep track of the myriad people who use these various online processes and platforms, companies have also resorted to more technologically-advanced

methods of collecting and storing user information. Namely, data collected from people signing up for email services, Facebook accounts, online banking profiles, retail rewards programs, and even employment records is all stored in "the cloud," an abstract vault under theoretical lock-and-key.[1] Just like any tangible system, the security measures in place for any one company's data storage system can be breached, exposing millions of peoples' data to cybercriminals who can manipulate and misuse this information.[2]

While many breaches never result in the public release of data,[3] and some go entirely undetected, remarkably few people ever actually know when their data has been breached—even after the affected service has publicly acknowledged an incident.[4] Data breaches are ever more present as the information economy places more value on data linked to individual users.[5] But plaintiffs have yet to find redress across federal courts, even when breached information could result in future identify theft.

---

[1] Quentin Hardy, *Where Does Cloud Storage Really Reside? And Is It Secure?*, N.Y. TIMES: ASK THE TIMES (Jan. 23, 2017), https://www.nytimes.com/2017/01/23/insider/where-does-cloud-storage-really-reside-and-is-it-secure.html.

[2] Jeff Elder, *A "Staggering" Failure to Adopt Basic Security Habits Led to 70% of Companies Storing Data with Amazon, Microsoft, or Other Big Cloud Vendors Getting Hacked or Exposing Data Last Year, Researchers Say*, BUS. INSIDER (July 8, 2020, 5:36 PM), https://www.businessinsider.com/cloud-computing-hacked-cybersecurity-sophos-amazon-2020-7.

[3] *See, e.g.*, Brendan I. Koerner, *Inside the Cyberattack that Shocked the US Government*, WIRED (Oct. 23, 2016, 5:00 PM), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/; *see also* Lily Hay Newman, *The Wired Guide to Data Breaches*, WIRED (Dec. 7, 2018, 9:00 AM), https://www.wired.com/story/wired-guide-to-data-breaches/?GuidesLearnMore ("Pilfered OPM data never circulated online or showed up on the black market, likely because it was stolen for its intelligence value rather than its street value. Reports indicated that Chinese operatives may have used the information to supplement a database cataloging US citizens and government activity.").

[4] In fact, this Author had never previously been notified of her information being exposed through a data breach until she investigated this herself using one of several legitimate websites. After inputting her email address into the website *Have I Been Pwned*, this Author discovered that personal information linked to this email address had been exposed in ten separate breaches over the course of a decade. This Author's personal story is not uncommon in America today. *See also* HAVE I BEEN PWNED?, https://haveibeenpwned.com (last visited Sept. 6, 2020). To check the security of an email address, readers can input their personal email into the search bar on this secure website's Home page and click the "pwned?" button. The website will then break down and explain any known data breaches that the email address has been involved in, including the type of breach. It is generally recommended that users subsequently change all passwords associated with an email address involved in a known breach. *See also* Lily Hay Newman, *All the Ways Equifax Epically Bungled Its Breach Response*, WIRED (Sept. 24, 2017, 9:00 AM), https://www.wired.com/story/equifax-breach-response/.

[5] Meera Jagannathan, *Data Breached Soared by 17% in 2019: "We Also Saw the Rise of a Significant New Threat"*, MARKETWATCH (Jan. 29, 2020, 6:07 AM), https://www.marketwatch.com/story/data-breaches-soared-by-17-in-2019-but-theres-some-good-news-too-2020-01-29.

This raises an important question: Is the risk of future identity theft (or other harm) enough to establish standing for plaintiffs to sue in federal court after a data breach? Most recently, there has been a split among United States circuit courts of appeals regarding this question. In *In re United States Office of Personnel Management Data Security Breach Litigation* (*In re U.S. OPM*),[6] the D.C. Circuit held that it was, siding with the Sixth,[7] Seventh,[8] and Ninth[9] Circuits in finding that plaintiffs alleging a risk of future harm can establish standing.[10] However, in *Beck v. McDonald*,[11] the Fourth Circuit recently held the opposite, joining the ranks of the Second,[12] Third,[13] and Eighth[14] Circuits in requiring plaintiffs to show more before standing is established.[15] Our increasingly technology-driven world has made data much more valuable, and even with strides being made in cybersecurity, data is now also more vulnerable to misuse when breaches occur.[16] However, the imminence of the threat of data misuse in the wake of a breach should not be held to the same stringent constitutional standard as other issues of imminence given that data can be accessed and stored for months or even years before it is used or "stolen." Rather, courts should weigh the devastating effects of identity theft in the 21st century more heavily against the imminent threat requirement to better protect plaintiffs seeking justice in the wake of a data breach.

Yet individual state data protection laws vary, leading to inconsistencies and a lack of uniformity regarding data breach victims' rights. Luckily, the United States has new guidance available. The European Union ("EU") recently adopted the General Data Protection Regulation ("GDPR" or "the Regulation"), a sweeping regulatory framework which aims to protect all EU citizens from data and privacy breaches and imposes strict standards on all companies that process EU citizens' data, regardless of the company's location.

---

6 928 F.3d 42 (D.C. Cir. 2019) [hereinafter *In re U.S. OPM*].

7 *See* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016).

8 *See* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016); Remijas v. Neiman Marcus Grp., L.L.C., 794 F.3d 688 (7th Cir. 2015); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007).

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

10 *In re U.S. OPM*, 928 F.3d at 75.

11 848 F.3d 262 (4th Cir. 2017).

12 Whalen v. Michaels Stores, Inc., 689 Fed. App'x 89 (2d Cir. 2017).

13 Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

14 *See In re* SuperValu, Inc., 870 F.3d 763 (8th Cir. 2017).

15 *Beck*, 848 F.3d at 272.

16 *See* Michael Grothaus, *How Our Data Got Hacked, Scandalized, and Abused in 2018*, FAST CO. (Dec. 13, 2018), https://www.fastcompany.com/90272858/how-our-data-got-hacked-scandalized-and-abused-in-2018.

This Note will identify the implication of the current standing doctrine on plaintiffs' rights in data breach cases and how the European Union's GDPR can provide principles and guidance to adapt the American standing framework to the modern era. After identifying the ways in which the GDPR affords citizens more rights for redress post-breach, this Note will posit that the U.S. should adopt a framework to update constitutional standards and show why such a standard will work for the American legal system. Accordingly, this Note aims to provide the Supreme Court and Congress with a new method of analysis for framing the need for uniform standing rules across the United States, specifically in relation to data breach litigation. By adopting a uniform rule, the U.S. can create a system that is beneficial to both sides. Not only would companies be deterred from engaging in behavior that might lead to breaches in the future, but, also, the affected plaintiffs would be given an opportunity for recourse when breaches do occur.

In Part II, this Note first identifies the issue of the circuit split, providing background on several cases that have come down to standing as an issue—particularly as it relates to the imminence of a threat of data misuse. This Note then provides background on the EU's GDPR, underscoring the aspects of company regulation and citizens' rights that are most important for developing a framework for legal action under the U.S. Constitution. Part II ends with a brief review of international and domestic examples of laws that have used the GDPR as a model. In Part III, this Note will identify the benefits of following the GDPR while highlighting the pitfalls of allowing the circuits and individual states to develop limited frameworks to address data privacy and protection. Specifically, the U.S. must consider both international and domestic issues that point to the GDPR as a gold standard for data protection regulation. Part IV concludes, reiterating the need for a uniform federal framework that adequately protects consumer rights while incentivizing businesses to comply.

II. BACKGROUND

The following sections lay the foundation for the argument that the principles of the GDPR can be applied to an American constitutional framework for standing in data breach cases. Section A explains the role that Article III standing plays in bringing a cause of action under U.S. law, highlighting the primary issue that data breach plaintiffs face at the pleading stage. Next, Section B documents the circuit split in approaching the question of standing in several notable cases. Finally, Section C identifies the history and purpose of the GDPR before unpacking the clauses that are most relevant to organizations' obligations and plaintiffs' rights post-breach.

A. Article III Standing Doctrine

In order for a federal court to establish jurisdiction over any litigation,[17] a plaintiff must show that she has standing to sue,[18] meaning that the federal court has the power to adjudicate her case, regardless of the strength of the claim.[19] The doctrine of standing is derived from the Constitution's division of power between the legislative,[20] executive,[21] and judicial[22] branches.[23] While Article III of the Constitution restricts federal court jurisdiction to "cases" and "controversies," it does not expressly define these terms.[24] As a result, the Supreme Court has developed the doctrine of standing to both clarify the boundaries of justiciability under Article III and to reinforce the "proper . . . role of the courts in a democratic society."[25] Accordingly, to establish standing to sue in a federal court, a plaintiff must show (1) that she has suffered an injury-in-fact, (2) that the injury is fairly traceable to the defendant, and (3) that the injury is redressable by a favorable judicial decision.[26] In data breach litigation, the most difficult requirement for plaintiffs to meet has most often been establishing an injury-in-fact.

An injury-in-fact is "an invasion of a legally protected interest."[27] The injury must be "actual or imminent" and both "concrete" and "particularized."[28] First, the alleged injury must be either actual—that is, the injury has occurred or is ongoing—or it must be imminent.[29] Second, a concrete injury must be de facto;

---

17 Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 94–95 (1998) (quoting Mansfield, C. & L.M. Ry. Co. v. Swan, 111 U.S. 379, 382 (1884)) ("The requirement that jurisdiction be established as a threshold matter 'spring[s] from the nature and limits of the judicial power of the United States' and is 'inflexible and without exception.'").

18 *Id.* at 102.

19 *Id.* at 89; Bell v. Hood, 327 U.S. 678, 682 (1946) ("Jurisdiction . . . is not defeated . . . by the possibility that the averments might fail to state a cause of action on which petitioners could actually recover.").

20 U.S. CONST. art. 1, § 1.

21 *Id.* art. 2, § 1.

22 *Id.* art. 3, § 1.

23 *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 559 (1992).

24 *Id.*

25 Warth v. Seldin, 422 U.S. 490, 498 (1975).

26 *See Lujan*, 504 U.S. at 560–61.

27 *Id.* at 560.

28 Monsanto Co. v. Geerston Seed Farms, 561 U.S. 139, 149 (2010).

29 *Id.*

it must actually exist and cannot be merely abstract.[30] Third, a particularized injury "must affect the plaintiff in a personal and individual way."[31]

While it is understandably difficult for plaintiffs to show that a data breach actually exposed their private data in the first place, it is considerably more difficult for plaintiffs to prove that the harm to their privacy is imminent. Because the data cannot be shown to have already been misused in some situations, plaintiffs are left to allege that there remains a threat of *future* injury. However, "[a]n allegation of future injury" satisfies Article III only if it "is 'certainly impending,' or there is a 'substantial risk' that the harm will occur."[32]

B. The Circuit Split on Article III Standing in Data Breach Cases

The circuits have split in their approaches to Article III standing with regard to data breach plaintiffs.[33] In data breach cases, plaintiffs generally attempt to establish standing on the theory that they suffer an increased risk of identity theft following the breach.[34] This is referred to as "increased-risk standing," given the general inability to determine actual injury where the subject of litigation is personal property existing in cyberspace. In the wake of the Supreme Court's various takes on increased-risk standing in cases like *Clapper v. Amnesty International USA*[35] and *Spokeo, Inc. v. Robins*,[36] lower courts have reached different conclusions about whether such injuries satisfy the standing test.[37] These holdings have been generally fact-dependent, focusing on either the

---

30 Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016).

31 *Lujan*, 504 U.S. at 560 n.1.

32 Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014) (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 (2013)).

33 *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (denying standing for data breach plaintiffs); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (granting standing for data breach plaintiffs).

34 *See, e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (holding that the increased risk of identity theft was sufficient to confer standing).

35 568 U.S. 398, 410 (2013) (holding that plaintiffs lacked Article III standing because they alleged a risk of future harm).

36 136 S. Ct. 1540, 1548 (2016) (finding the Ninth Circuit's Article III standing analysis was incomplete because the court failed to consider the "concreteness" requirement of plaintiff's alleged injury).

37 *Compare* Beck v. McDonald, 848 F.3d 262, 272 (4th Cir. 2017) (denying standing based on the increased risk of identity theft arising out of two data breaches at a hospital, noting that the threat of identity theft was based on a "highly attenuated chain of possibilities" (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013))), *with* Remijas v. Neiman Marcus Grp., L.L.C., 794 F.3d 688, 693 (7th Cir. 2015) (granting standing after a data breach based on the increased risk of identity theft, noting that "[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities").

type of data that was stolen[38] or whether the data was targeted and understood by hackers.[39] However, these decisions also represent the circuits' general willingness or reluctance to recognize increased-risk standing, and, as such, they are useful in analyzing plaintiffs' standing specific to data breach cases.

1. Standing Granted

Across the circuits that have granted Article III standing to data breach victims, common themes can be traced throughout the courts' factual analyses of each case. Notably, these circuits focus on (1) the type of information exposed to cybercriminals and (2) the likelihood that such exposure necessarily presents a valid concern regarding the imminence of claimed threats of future harm.

For example, in *In re U.S. OPM*, one class of plaintiffs claimed to have suffered a variety of past and future data breach related harms in the wake of a cyberattack on a federal personnel records database.[40] Focusing on the plaintiffs' shared injury of risk of future identity theft,[41] the United States Court of Appeals for the District of Columbia Circuit found that there was "no question" that hackers gained access to "all the information needed to steal [the plaintiffs'] identities,"[42] in addition to finding that some plaintiffs had already experienced "various types of identity theft."[43] Reversing the district court's denial of standing to this class of plaintiffs, the court held that the proven instances of identity theft not only "illustrate[d] the nefarious uses to which [such] stolen

---

38 *See, e.g.*, *In re* SuperValu, Inc., 870 F.3d 763, 771–72 (8th Cir. 2017) (rejecting increased-risk standing for a class of plaintiffs whose credit and debit card information was stolen, but whose personal identifying information was not stolen).

39 *See, e.g.*, *Beck*, 848 F.3d at 275 (declining to assume that thieves targeted stolen laptops for the personal information they contained); *see also* Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011) (rejecting increased-risk standing after a hacker penetrated a payroll system firewall because it was "not known whether the hacker read, copied, or understood" the system's information).

40 For example, one plaintiff allegedly suffered stress "resulting from concerns for her personal safety and that of her family members" after being informed by the FBI that her personal identifying information "had been acquired by the so-called Islamic State of Iraq and al-Sham ('ISIS')." *In re U.S. OPM*, 928 F.3d 42, 55 (D.C. Cir. 2019) (citing Arnold Plaintiffs' Compl. ¶ 22).

41 The D.C. Circuit has previously recognized the risk of future identity theft as a "concrete and particularized" injury for the purposes of Article III standing. Attias v. Carefirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017); *see also* Hancock v. Urb. Outfitters, Inc., 830 F.3d 511, 514 (D.C. Cir. 2016) (presenting the "increased risk of fraud or identity theft" as an "example" of a "concrete consequence" for standing purposes).

42 *In re U.S. OPM*, 928 F.3d at 56 ("[T]he hackers [allegedly] stole Social Security numbers, birth dates, fingerprints, and addresses, among other sensitive personal information. It hardly takes a criminal mastermind to imagine how such information could be used to commit identity theft.").

43 *Id.* (referring to the "unauthorized opening of new credit card and other financial accounts and the filing of fraudulent tax returns in [the affected plaintiffs'] names").

information may be put," but that such instances also supported "the inference that [the plaintiffs] face[d] a substantial—as opposed to a merely speculative or theoretical—risk of future identity theft."[44] The D.C. Circuit had previously granted standing on the issue in 2017, finding that "a substantial risk of harm exist[ed] already, simply by virtue of the hack and the nature of the data that the plaintiffs allege[d] was taken."[45]

Similarly, the Sixth Circuit has held Article III standing is satisfied in data breach cases where the nature of the information breached raises concern for the plaintiffs.[46] In *Galaria v. Nationwide Mutual Insurance Co.*,[47] plaintiffs brought various claims, including alleged violations of the Federal Credit Reporting Act ("FCRA"), that stemmed from a 2012 data breach where the personal information of over one million Nationwide customers was allegedly impacted.[48] The Sixth Circuit reversed the district court's partial dismissal of the case, finding that the increased risk of identity fraud constituted sufficient pleading of injury under Article III.[49] The court highlighted that "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for . . . fraudulent purposes."[50]

---

[44] *Id.* ("[U]nlike existing credit card numbers, which, if compromised, can be changed to prevent future fraud, Social Security numbers and addresses cannot so readily be swapped out for new ones. And, of course, our birth dates and fingerprints are with us forever."); *see also id.* at 57 ("Cyber-hacking on such a massive scale is a relatively new phenomenon, and we are unwilling at this stage to assume that the passage of a year or two without any clearly identifiable pattern of identity theft or financial fraud means that all those whose data was compromised are in the clear.").

[45] *Attias*, 865 F.3d at 629 (reversing the district court's dismissal for lack of standing where plaintiffs in a class action suit against a health insurance company alleged that a data breach compromised their personal identifying information). Specifically, the plaintiffs alleged that the breach exposed "all of the information wrongdoers need for appropriation of a victim's identity": personal identification information, credit card numbers, and Social Security numbers. *Id.* at 628 (internal quotation marks omitted); *see also In re U.S. OPM*, 928 F.3d at 55–56 ("Based largely on the nature of the information compromised in the attack [in *Attias*], we concluded that it was reasonable to infer that the cyberattackers had 'both the intent and the ability to use that data for ill.'" (internal citation omitted)). Ultimately, the court found that the plaintiffs had "cleared the low bar to establish their standing at the pleading stage" by plausibly alleging that they faced a substantial risk of identity theft as a result of the company's negligent failure to prevent the breach. *Attias*, 865 F.3d at 622.

[46] Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016).

[47] 663 F. App'x 384 (6th Cir. 2016).

[48] *Id.* at 386.

[49] *Id.* at 388–89.

[50] *Id.* at 388.

The Seventh and Ninth Circuits have also recognized standing in several data breach cases.[51] In *Remijas v. Neiman Marcus Group, L.L.C.*,[52] the plaintiffs brought various claims stemming from a 2013 breach that compromised information from approximately 350,000 customers' credit cards, 9,200 of which were found to have been used fraudulently.[53] The Seventh Circuit reversed the district court's dismissal, finding the plaintiffs had demonstrated an "objectively reasonable likelihood" that harm would occur, and the plaintiffs had adequately alleged standing under Article III.[54] Perhaps the most important observation of all the cases in this section, the court reasoned here that "customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing."[55]

More recently, in *In re Zappos.com, Inc.*,[56] class action plaintiffs brought suit in the Ninth Circuit over a 2012 incident that allegedly resulted in the compromise of personal information from Zappos' customers.[57] Here, the district court held that only plaintiffs claiming to have already suffered financial losses resulting from the breach had standing to sue.[58] On appeal, the Ninth Circuit reversed, holding instead that even those plaintiffs who had only alleged "imminent" financial losses also had sufficient standing to sue because "substantial risk that the harm will occur" is sufficient to plead the injury requirement for standing under Ninth Circuit precedent.[59]

2. Standing Denied

Circuits on the other side of the split have applied a much narrower methodology regarding the pleading standards for an Article III injury-in-fact, despite these cases involving the same types of sensitive information as discussed in the previous section. Notably, these courts have been less likely to recognize the threat of future harm or future risk of identity theft, especially where plaintiffs have not yet experienced specific instances of harm.

---

51 *In re* Zappos.com, Inc., 888 F.3d 1020 (9th Cir. 2018); Remijas v. Neiman Marcus Grp., L.L.C., 794 F.3d 688 (7th Cir. 2015); Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007).

52 794 F.3d 688 (7th Cir. 2015).

53 *Id.* at 690.

54 *Id.* at 693 ("Why else would hackers break into a . . . database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.").

55 *Id.*

56 888 F.3d 1020 (9th Cir. 2018).

57 *Id.* at 1023.

58 *Id.* at 1024.

59 *Id.* at 1025–26.

In *Beck v. McDonald*, a laptop containing patients' unencrypted personal information and several boxes of medical records went missing from a South Carolina Veterans Affairs medical center on two separate occasions in 2013 and 2014, respectively.[60] The Fourth Circuit affirmed the district court's dismissal of these claims, holding that the increased risk of future harm of identity theft was insufficient to demonstrate injury-in-fact and specifically noting that the inability to point to a proven instance of identity theft three to four years after the breaches in question illustrated the "speculative" nature of the plaintiffs' claimed injuries.[61] In contrast, in 2018, the Fourth Circuit reversed a district court's dismissal of a complaint on standing grounds because the plaintiffs could point to specific instances where their personal information had been used fraudulently.[62]

A comparable case, *In re SuperValu, Inc.*,[63] centered on a plaintiff's allegations that a 2014 breach resulted in the compromise of credit card and personal information belonging to SuperValu customers.[64] Here, the Eighth Circuit affirmed the district court's dismissal, stating that plaintiffs could not "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[65] However, one plaintiff was allowed to proceed with his claims by alleging fraudulent charges had already been made to his credit card account following the breach.[66]

In *Reilly v. Ceridian Corp.*,[67] the Third Circuit affirmed a district court's dismissal of a case involving the breach of a payroll processing firm's database because plaintiffs could only show a "hypothetical, future injury" that was insufficient to demonstrate standing.[68] Rather, the court held that plaintiffs would have to present evidence that the personal information allegedly exposed had been "read, copied, and understood" and subsequently used "successfully" by the "hacker."[69] More recently, the Third Circuit reversed a district court's dismissal of data breach litigation on standing grounds in *In re Horizon*

---

60 *Id.* at 267–69. The information on the laptop included patients' "names, birth dates, the last four digits of social security numbers, and physical descriptors," while the boxes of medical records contained patients' names and social security numbers. *Id.*

61 Without such allegations, the Fourth Circuit explained, there was nothing to "push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent." *Id.* at 274.

62 Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc., 892 F.3d 613, 622 (4th Cir. 2018).

63 870 F.3d 763 (8th Cir. 2017).

64 *Id.* at 766–67.

65 *Id.* at 771 (citing Clapper v. Amnesty Int'l USA, 586 U.S. 398, 415 (2013)).

66 *Id.* at 772–74.

67 664 F.3d 38 (3d Cir. 2011).

68 *Id.* at 42–43.

69 *Id.*

Healthcare Services Inc. Data Breach Litigation,[70] holding that plaintiffs successfully pled a de facto concrete injury-in-fact due to defendant Horizon's alleged statutory violation.[71]

Finally, the Second Circuit aligned with the other courts in this section when it held in *Whalen v. Michaels Stores, Inc.*,[72] that the district court properly dismissed a case for lack of standing because the plaintiff had not suffered a "particularized and concrete injury" where fraudulent charges had been reimbursed following a 2014 data breach affecting credit card information belonging to Michaels Stores' customers.[73] The court further observed that the plaintiff could not plausibly allege a risk of future harm when her credit card had been promptly cancelled and no other personal information had been claimed as stolen after the breach.[74]

Despite the circuit courts of appeals' failure to reach a clear consensus on the issue of standing specific to data breach plaintiffs, the Supreme Court has thus far declined to clarify this issue.[75] After denying a petition for certiorari in the Fourth Circuit's *Beck* case in June 2017,[76] the Court denied another petition for certiorari in *Attias v. CareFirst, Inc.*[77] during the 2017–18 term, permitting the D.C. Circuit's holding to stand as well. Recently, the Court denied a petition for certiorari regarding the Ninth Circuit's *In re Zappos.com, Inc.* case in March 2019.[78] Consequently, holdings from both sides of the split remain good law, keeping all present and future litigants bound to the whims of the circuits.

C. The European Union's General Data Protection Regulation

In May 2018, the GDPR entered into force across the EU.[79] The Regulation applies to (1) all companies or entities which process personal data as part of the activities of one of their branches established in the EU, regardless of where the data is processed; or (2) companies established outside the EU that offer goods and/or services (paid or for free) or that monitor the behavior of

---

70 846 F.3d 625 (3d Cir. 2017).

71 *Id.* at 635.

72 689 Fed. App'x 89 (2d Cir. 2017).

73 *Id.* at 90.

74 *Id.*

75 *See, e.g.*, Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016).

76 *See* Beck v. McDonald, 848 F.3d 262, 268 (4th Cir. 2017), *cert. denied sub nom.* Beck v. Shulkin, No. 16-1328, 2017 WL 1740442 (U.S. June 26, 2017).

77 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018) (Mem.).

78 *In re* Zappos.com, Inc., 888 F.3d 1020 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019).

79 Ben Wolford, *What Is the GDPR, the EU's New Data Protection Law?*, GDPR, https://gdpr.eu/what-is-gdpr/?cn-reloaded=1 (last visited Sept. 23, 2020).

individuals in the EU.[80] However, if processing personal data does not constitute a core part of the business *and* the activity does not create risks for individuals, then some obligations of the GDPR do not apply to the company.[81] Processing personal data is regarded as one of a company's "core activities" where it forms "an inextricable part of the controller's or processor's activities."[82]

Under the Regulation, a "personal data breach" is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."[83] One of the most relevant aspects of the GDPR to the American legal system is that "data subjects"—people whose data is processed by a company subject to the Regulation—are recognized as having a right to be provided with effective and enforceable rights and effective administrative and judicial redress both before, during, and after a breach occurs. This concept is expressly included throughout the Regulation. For example, in the Regulation's preamble, the Drafters acknowledge that data breaches may result in "physical, material or non-material damage" to data subjects, such as "loss of control over personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage."[84]

Not only are data breach victims' potential harms outlined as an underlying purpose for the Regulation's rules on data processing companies, but companies' obligations to notify both an authoritative body and breach victims about a breach are also enumerated within Articles 33 and 34, respectively.

Under Article 33, in the event of a personal data breach the data "controller," or company that possessed the data, must notify a supervisory authority about the breach "without undue delay and, where feasible, not later than 72 hours after having become aware of [the breach]."[85] This is the default rule under the Regulation, unless the breach is "unlikely to result in a risk to the

---

[80] *Who Does the Data Protection Law Apply To?*, EUROPEAN COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en (last visited Sept. 6, 2020).

[81] *See id.* For example, the appointment of a Data Protection Officer ("DPO") would not apply to a company whose "core activities" do not include processing personal data and where the company's activities do not create risks for individuals. *Id.*

[82] *Id.*

[83] General Data Protection Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, 34 (EU) [hereinafter GDPR].

[84] *Id.* ¶ 85.

[85] *Id.* art. 33(1).

rights and freedoms of natural persons."[86] If the notification is not made within 72 hours, the company must additionally communicate the reasons for the delay.[87] Where the breach is first discovered by an entity designated as the "processor" for the controlling company, the processor "shall notify the controller without undue delay after becoming aware of [the breach]."[88] It is also important to note that these notifications must be detailed to some extent,[89] and when companies are unable to communicate all required information at once, they are permitted to release details in phases so as to remain in compliance with the Regulation without needlessly delaying the process of redress.

Under Article 34, a data controller is obliged to communicate data breaches to victims "without undue delay" when such a breach "is likely to result in a high risk to the [victims'] rights and freedoms."[90] The notification to the victim is required to describe "in clear and plain language" the nature of the breach, and, while it does not have to outline the overarching statistical information related to the breach, it should at least

> (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.[91]

However, companies are still given a degree of leeway in the notification process regarding victim communication. Specifically, no notification is required if "appropriate technical and organizational protection measures" such as encryption were in place and applied to the data affected by the breach; subsequent measures were taken to mitigate the likelihood of "high risk to the

---

86 *Id.*

87 *Id.*

88 *Id.* art. 33(2).

89 *Id.* art. 33(3). Specifically, the notification to the supervisory authority must:

> (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Id.

90 *Id.* art. 34(1).

91 *Id.* art. 34(2).

rights and freedoms" of victims; or where such notification would involve "disproportionate effort."[92] As a last resort, should a company have failed to communicate information regarding a breach to victims, the supervisory authority, "having considered the likelihood of the personal data breach resulting in a high risk,"[93] may require the company to fulfill its obligations or may determine that the notification is not required under the Regulation. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.[94]

After the notification process has been carried out, eligible breach victims are afforded the right to compensation under Article 82, regardless of whether the damage suffered was material or non-material.[95] In addition, *any* data controller involved in processing shall be liable for the damage caused where it has not complied with its obligations under the Regulation or where it has acted outside or contrary to lawful instructions of the controller.[96] A controller or processor is "exempt from liability . . . if it proves that it is not in any way responsible for the event giving rise to the damage."[97] In the event that more than one controller or processor (or both a controller and a processor) are involved in the same processing and where they are responsible for any damage caused by processing, *each entity is held liable for the entirety of the damage* caused "to ensure effective compensation of the data subject."[98] Finally, where one controller or processor has fully compensated victims for the damage suffered, that controller or processor becomes legally entitled to make a compensatory claim against the other controllers or processors involved in the incident, proportional to each party's responsibility.[99]

---

92 *Id.* art. 34(3). In cases where disproportionate effort would be required on the part of the company to notify breach victims, a public communication or similar measure whereby victims are informed in an equally effective manner is instead required. *Id.*

93 *Id.* art. 34(4).

94 *Id.* ¶ 86.

95 *Id.* art. 82(1).

96 *Id.* art. 82(2).

97 *Id.* art. 82(3).

98 *Id.* art. 82(4). This style of shared liability could be especially effective in the U.S. torts system, where it is helpful for defendants to show that a breach was the result of multiple actors, thereby reducing the cost of settlement. *See infra* Section III.A.2.

99 GDPR, *supra* note 83, art. 82(5). Again, this clause closely resembles the U.S. civil tort system, where defendants sharing liability can become indebted to one defendant who fully compensated the plaintiffs for events resulting from all defendants' negligent acts. *See infra* Section III.A.2.

D. International Iterations of the GDPR

Since it took legal effect in 2018, the GDPR has emerged as a reference point and acted as a catalyst for many countries around the world contemplating how to modernize their privacy rules. These include Chile,[100] South Korea,[101] Japan,[102] Kenya,[103] Tunisia,[104] Indonesia,[105] and Taiwan,[106] to name just a few. International instruments, such as the modernized "Convention 108" of the Council of Europe,[107] or the "Data Free Flow with Trust" initiative launched by Japan[108] are also based on principles that are shared by the GDPR. Notably, Brazil and India, key players on the international stage, have also promulgated laws that tailor the GDPR framework to their domestic goals. Because each of these countries is comparable to the U.S. in size and international stature, this section briefly describes each country's iteration of the GDPR framework.

---

[100] *See Data Protection Laws of the World: Chile*, DLA PIPER, https://www.dlapiperdataprotection.com/index.html?t=law&c=CL (Jan. 14, 2020).

[101] Chris H. Kang, Sun Hee Kim & Doil Son, *Korea Introduces Major Amendments to Data Privacy Laws*, LEXOLOGY (Jan. 30, 2020), https://www.lexology.com/library/detail.aspx?g=223051e2-0346-4935-8fbb-6146e4424d94.

[102] Hiroto Imai, Kyle Reykalin & Mitsuhiro Yoshimura, *Update of Japan's Privacy Law Approved by Cabinet*, HOGAN LOVELLS: ENGAGE (Mar. 31, 2020), https://www.engage.hoganlovells.com/knowledgeservices/news/update-of-japans-privacy-law-approved-by-cabinet.

[103] George Obulutsa & Duncan Miriri, *Kenya Passes Data Protection Law Crucial for Tech Investments*, REUTERS (Nov. 8, 2019, 8:52 AM), https://www.reuters.com/article/us-kenya-dataprotection/kenya-passes-data-protection-law-crucial-for-tech-investments-idUSKBN1XI1O1.

[104] Henning Haake, *The GDPR's Extra-Territorial Reach – Data Protection in Tunisia*, EUROFORUM (Mar. 1, 2017), https://www.euroforum.de/edpd/gdpr-extra-territorial-reach-data-protection-tunisia/.

[105] Michael S. Carl & Revaldi N. Wirabuana, *With GDPR as Guide, Indonesia Nears Major Changes to Rights of Personal Data Owners*, LEXOLOGY (June 8, 2020), https://www.lexology.com/library/detail.aspx?g=46380fe5-c18e-497a-bda1-39f68c88b490.

[106] Central News Agency, *EU Lauds Taiwan's Efforts To Push for Talks on Data Transfer Deal*, TAIWAN NEWS (Mar. 11, 2019, 6:01PM), https://www.taiwannews.com.tw/en/news/3655633.

[107] *See* COUNCIL OF EUR. TREATY OFF., *Details of Treaty No.108: Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data*, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (last visited Sept. 6, 2020).

[108] WORLD ECON. F., DATA FREE FLOW WITH TRUST (DFFT): PATHS TOWARDS FREE AND TRUSTED DATA FLOWS (2020), http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf.

1. Brazil's General Data Protection Law

Brazil's Lei Geral de Proteção de Dados[109] ("LGPD"), passed shortly after the GDPR in 2018, attempts to unify over 40 different statutes that currently govern personal data—both online and offline. This unification of previously disparate and oftentimes contradictory regulations is only one similarity it shares with its inspiration, the EU's GDPR.[110] In addition to its purpose, the LGPD follows the GDPR in that it applies to any entity that processes Brazilians' personal data, regardless of where that business or organization might actually be located.[111] Furthermore, the LGPD provides data subjects with essentially the same fundamental rights as the GDPR.[112] While the LGPD does distinguish between "personal data" and "*sensitive* personal data,"[113] it appears to take a more expansive approach than the GDPR with regard to what can constitute personal data. In various places throughout the text, the law states that personal data can mean *any* data that, by itself or combined with other data, could identify a natural person or subject them to a specific treatment.

Though the LGPD and GDPR are quite similar in various ways, they diverge in three key areas. First, the GDPR has six lawful bases for processing,[114] and a data controller must choose one of them as a justification for using a data subject's information. However, the LGPD lists ten,[115] notably including the protection of credit as a legal basis for the processing of data, which is a substantial departure from the GDPR. Second, the laws vary in their requirements for reporting of data breaches. While both laws require entities to report data breaches to a local data protection authority, the level of specificity varies widely. The GDPR is explicit: an organization must report a data breach within 72 hours of its discovery.[116] In contrast, the LGPD does not give a firm deadline: breaches must be communicated merely within a reasonable time

---

109 Lei Geral de Proteção de Dados Pessoais (General Data Protection Law), Law No. 13,709/2018, [hereinafter LGPD], https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf (last visited Sept. 6, 2020).

110 Richie Koch, *What Is the LGPD? Brazil's Version of the GDPR*, GDPR.EU, https://gdpr.eu/gdpr-vs-lgpd/?cn-reloaded=1 (last visited Sept. 6, 2020).

111 LGPD, *supra* note 109, art. 3.

112 *Id.* art. 18. While the GDPR is known for granting its data subjects eight fundamental rights, they are essentially the same rights the LGPD mentions. The LGPD grants nine fundamental rights, appearing to distinguish "[t]he right to information about public and private entities with which the controller has shared data" from the GDPR's more general "[r]ight to be informed" to make this right more explicit.

113 *Id.* art. 5(I)–(II) (emphasis added).

114 GDPR, *supra* note 83, Recital 40, art. 6.

115 LGPD, *supra* note 109, art. 7.

116 GDPR, *supra* note 83, art. 33.

period.[117] This will be left to the national regulating body to further define the scope of "reasonable." Finally, there is a stark contrast in the laws' maximum fines imposed on violating entities. The GDPR famously imposes substantial maximum fines,[118] while the LGPD's maximum fines are only half as much.[119]

2. India's Proposed Personal Data Protection Bill

In 2017, India's Supreme Court established a constitutional right to privacy.[120] A first draft of India's proposed Personal Data Protection Bill ("PDPB")[121] soon followed in late 2019. Like the GDPR, in practice, India's bill would require global internet companies like Facebook and Amazon to seek explicit permission for most uses of an individual's personal data and make it easier for people to demand that their data be erased.[122] While the data protection rules would apply to government agencies as well as private companies, the law would still grant the central government power to exempt any public entity from these requirements for reasons such as national security or public order.[123] The PDPB also proposes a new entity, the Data Protection Authority, to write specific rules, monitor how corporations are applying them and settle disputes.[124] Interestingly, the PDPB would also require critical personal data to be stored on servers within India, with constraints on the transfer of other personal data outside India.[125]

Though the PDPB imposes typical penalties that include the prohibition of data processing and financial consequences for noncompliance,[126] it differs from the GDPR in some respects. Most significantly, the bill not only provides for criminal penalties for harms arising from violations,[127] but it also proposes to treat the relationship between a data processor and its consumer as "fiduciary."[128]

---

117 LGPD, *supra* note 109, art. 48 ("[T]he controller must communicate to the national authority and to the data subject the occurrence of a security incident that may create risk or relevant damage to the data subjects . . . in a reasonable time period, as defined by the national authority.").

118 *Infra* Section III.A.

119 *See* LGPD, *supra* note 109, art. 52. The maximum fine for a violation is "2% of a private legal entity's, group's, or conglomerate's revenue in Brazil, for the prior fiscal year, excluding taxes, up to a total maximum of 50 million reals." *Id.*

120 Geeta Pandey, *Indian Supreme Court in Landmark Ruling on Privacy*, BBC (Aug. 24, 2017), https://www.bbc.com/news/world-asia-india-41033954.

121 The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, (India).

122 *See id.* cl. 7, 11, 20.

123 *See id.* cl. 35–40.

124 *See id.* cl. 41–56.

125 *Id.* cl. 33–34.

126 *Id.* cl. 57–61.

127 *Id.* cl. 82.

128 *Id.* cl. 3(13).

E. The California Consumer Privacy Act

While the U.S. is free to take notes from Brazil and India's developing legal frameworks, there is a version of the GDPR that is much closer to home, and which will likely provide the best foundation for building up a national framework modeled after the GDPR. The California Consumer Privacy Act ("CCPA" or "the Act") officially took effect on January 1, 2020.[129] Originally enacted in 2018, the CCPA creates new consumer rights for California citizens relating to the access to, deletion of, and sharing of personal information collected by businesses.[130] While the CCPA and the GDPR are separate legal frameworks with different scopes, definitions, and requirements, the CCPA reflects a significant number of provisions and goals already present in the GDPR. Namely, the Act grants consumers

> [t]he *right to know* what personal information is collected, used, shared or sold, both as to the categories and specific pieces of personal information;
> [t]he *right to delete* personal information held by businesses and by extension, a business's service provider;
> [t]he *right to opt-out* of sale of personal information. . .[; and]
> [t]he *right to non-discrimination* in terms of price or service when a consumer exercises a privacy right under [the Act].[131]

Like the GDPR, the CCPA only applies to businesses that meet certain criteria regarding revenue and data control. Specifically, a business will be subject to the CCPA if it (1) generates "annual gross revenues in excess of [$25 million]"; (2) "buys, receives . . . sells, or shares . . . the personal information of 50,000 or more consumers, households, or devices"; and/or (3) "derives 50[%] or more of its annual revenues from selling consumers' personal information."[132] California State Attorney General Xavier Becerra's final proposed draft regulations also seek to impose additional obligations on businesses that collect and manage the personal information of more than ten million consumers.[133] Just

---

[129] CAL. CIV. CODE §§ 1798.100–80 (West 2020).

[130] For a further breakdown of the CCPA and the ways in which consumers may take advantage of their rights under the new law, see Geoffrey A. Fowler, *Don't Sell My Data! We Finally Have a Law for That*, WASH. POST (Feb. 19, 2020), https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq/?arc404=true.

[131] *CCPA Fact Sheet*, CAL. DEP'T OF JUST., https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf (last visited Oct. 24, 2020).

[132] CAL. CIV. CODE § 1798.140(c)(1)(A)–(C).

[133] Namely, throughout the proposed regulations, the California Attorney General imposes an obligation on companies to retain certain documentation regarding CCPA compliance from consumer requests to documentation of compliance for some period of time; often two years. However, the proposed regulations also create an affirmative reporting requirement for a business

like the GDPR, the CCPA applies to California companies and any out-of-state entities whose business touches California consumers.[134]

However, the CCPA stands firmly apart from the GDPR in several ways. First, the law does not require companies to minimize the amount of data they collect in the first place.[135] In addition, companies do not have to share information with consumers that is already public, that has been collected in a job interview, or that has been aggregated in ways that do not identify individual consumers.[136] And businesses already covered by some existing privacy laws are exempt—even if those laws don't require the same transparency as the CCPA.[137] Significantly, the CCPA does not create an individual claim to file a lawsuit against a company that violates consumers' privacy rights. For now, only the California attorney general may bring a claim to enforce the CCPA,[138] a fact that is lamentable from a consumer advocacy perspective.

III. PRACTICAL ARGUMENTS FOR NATIONAL UNIFORMITY

A. The GDPR as the Gold Standard of Data Protection

Given the GDPR's status as a newly-enacted law, there is limited case law showing how the Regulation has been applied in the specific context of data breach cases. In almost all of these cases, massive fines have been leveled against companies that were found to have failed in taking the appropriate measure to adequately protect consumers' stored data.[139] The maximum GDPR fines are

---

that "alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of" ten million or more consumers. Companies that do so must compile metrics related to (1) the number of requests to know that the business received, complied with and denied; (2) the number of requests to delete the business received, complied with and denied; (3) the number of requests to opt-out received, complied with and denied; and (4) the median number of days within which the business substantively responded to each request. These metrics then must be reported either in a company's privacy policy or otherwise posted on the company website with a link to the separate page in the privacy policy. *See* CAL. CODE REGS. tit. 11, § 999.317(g) (2020). The text of the final proposed regulations is more easily accessible through the Attorney General's website at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf.

134 CAL. CIV. CODE § 1798.140(g).

135 *Id.* § 1798.100(b).

136 *Id.* §§ 1798.140(o)(2), 1798.145(a)(5).

137 *Id.* § 1798.145(c)–(f). These laws include the federal GLBA and HIPAA, meaning that banks and doctor's offices generally do not have to abide by the CCPA because they are already subject to a national privacy law. *See infra* Section III.C.1.

138 CAL. CIV. CODE § 1798.150(b).

139 *See* Vera Cherepanova, *GDPR Enforcement Report (May 2019),* FCPA BLOG (May 14, 2019, 8:18 AM), https://www.fcpablog.com/blog/2019/5/14/gdpr-enforcement-report-may-2019.html; Oliver Schmidt, *Germany's First Fine Under the GDPR Offers Enforcement Insights*,

substantial, requiring organizations that commit "grave" GDPR violations to pay to up to € 20 million or 4% of their annual global revenue, whichever is higher.[140]

In practice, these outcomes and other enforcement measures have appeared to serve as a deterrent for companies that are non-compliant in some way, while showing breach victims just how valuable their data is worth and validating a consumer's right to maintain some kind of control over his or her data. It is no wonder that the GDPR has been referred to as the "gold standard" for data privacy rights enforcement.[141]

B. Applying the GDPR to the Federal Circuit Split

If the U.S. were already following such principles of deterrence, coupled with uniform and concrete rights for data subjects, there likely would not be a circuit split with regard to whether consumers have standing in data breach cases. Defendant businesses would have hopefully been deterred by such a high potential fine for noncompliance, for one. In addition, even if the breaches had still occurred, affected consumers would have been able to exercise clearer rights with regard to protecting their data and receiving appropriate remedy. Most importantly, a federal law allowing consumers to bring a cause of action for a business's failure to timely notify them of the breach—for example—would have created a clear basis for Constitutional standing by statutorily recognizing the threat of data misuse as an imminent and concrete injury-in-fact.

A GDPR-type framework does not only benefit victims of breaches but can also provide some support for defendant data collectors that use third-party processors. For instance, the GDPR provides for liability-sharing where multiple defendants may be at fault for failure to comply with different aspects of the law, resulting in a breach.[142] Liabilty-sharing is not a new concept to the U.S. torts system, where defendants can sometimes reduce the cost of settlement or the impact of an unfavorable verdict by showing that a cause of action was the result of multiple actors' negligent activities, thereby escaping the full brunt of liability.[143] In data breach cases, where the penalties associated with noncompliance are more often than not massive fines, this aspect of the data privacy framework would likely be a welcome addition to federal U.S. law.

IAPP.ORG (Nov. 27, 2018), https://iapp.org/news/a/germanys-first-fine-under-the-gdpr-offers-enforcement-insights/.

140 Ben Wolford, *What Are the GDPR Fines?*, GDPR.EU, https://gdpr.eu/fines/ (last visited Sept. 6, 2020).

141 HIMSS TV, *GDPR is Gold Standard for How Companies Should Be Governing Data*, MOBI HEALTH NEWS (Mar. 25, 2019, 8:53 AM), https://www.mobihealthnews.com/content/gdpr-gold-standard-how-companies-should-be-governing-data.

142 *See* GDPR, *supra* note 83, art. 82(4), (5).

143 RESTATEMENT (THIRD) OF TORTS § 17 (AM. L. INST. 2000).

C. Other Domestic Considerations

Aside from the lessons that can be learned from directly applying the European GDPR to American case law, the U.S. could additionally learn from domestic laws, state developments, and current business practices that all point to the practicality of adopting a national framework for the protection of private consumer data. First, the U.S. already applies national standards to financial and medical information that are fairly similar to those regulated by the GDPR.[144] Second, the entry into force of California's new Consumer Privacy Act may inspire other impatient states to take legal action within their own jurisdictions to protect consumers' data—with the potential to add to the confusion and injustice already created by the circuit split. Finally, because the GDPR applies to *all* businesses whose data collection practices affect EU citizens, many American entities already have measures in place to ensure their compliance with the Regulation.[145] With the addition of new state laws creating similar-yet-different rules for these same businesses to catch up with, it seems more practical now than ever for the U.S. to adopt a uniform, national framework that mirrors what has already been done while making it easier for businesses to remain compliant with American law.

1. Current Legal Standards for Financial and Medical Information

Although there is currently no general federal security breach notification law, the U.S. has enacted laws pertaining to the privacy and security of personal information in the areas of financial institutions and medical information, as well as adopted security breach notification regulations for both of these industries.

Congress enacted the Gramm-Leach-Bliley Act ("GLBA")[146] in an effort to ensure that financial institutions adequately protect consumers' personal financial information. The GLBA restricts such institutions from disclosing financial information to third parties without providing notification to consumers.[147] Pursuant to the GLBA, the Office of the Comptroller of Currency, the Board of Governors of the Federal Reserve, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision promulgated the Interagency Guidance on Response Programs for Unauthorized Access to Customer

---

144 STEPHEN P. MULLIGAN, WILSON C. FREEMAN & CHRIS D. LINEBAUGH, CONGRESSIONAL RESEARCH SERV., DATA PROTECTION LAW: AN OVERVIEW 7–12 (2019).

145 *See GDPR Compliance Checklist for US Companies*, GDPR.EU, https://gdpr.eu/compliance-checklist-us-companies/ (last visited Sept. 24, 2020); *infra* Section III.C.3.1.

146 *See* 15 U.S.C.A. §§ 6801–09 (West 2020).

147 *Id.* § 6802.

Information and Customer Notice,[148] which is very similar to most current state security breach notification laws. However, because it is a federal regulation, it is not really limited in scope or jurisdiction, unlike state laws and circuit precedent.

The Department of Health and Human Services ("DHHS") has issued comparable regulations requiring health care providers, health plans and other entities covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[149] to notify individuals if their personal health information has been breached.[150] In this context, a breach is defined as the "acquisition, access, use, or disclosure of protected health information, which poses a significant risk of financial, reputational, or other harm to an individual."[151] Furthermore, the Federal Trade Commission ("FTC") promulgated the Health Breach Notification Rule, which applies specifically to foreign and domestic vendors of personal health records, related entities, and third-party service providers that maintain information belonging to U.S. citizens or residents.[152] The FTC's notification procedure and requirements essentially mirror the DHHS regulations, except notification is to be made to the FTC.[153] A violation of this rule is considered an unfair or deceptive act or practice in violation of the Federal Trade Commission Act regarding unfair or deceptive acts or practices.[154]

2. Extending CCPA Rights Beyond California

The CCPA really only applies to businesses whose data collecting processes touch and concern California residents, but this has not stopped some businesses from individually choosing to extend these rights beyond California's borders. For example, businesses like Netflix, Microsoft, Starbucks and United Postal Service are extending CCPA rights to all Americans.[155] This makes sense: it takes additional time and resources for companies to attempt to confirm where their consumers live, and it is far easier for a business to broadly apply a law like the CCPA rather than attempt to implement separate policies and procedures for monitoring a restricted class on consumers. Perhaps more obviously, it would be hypocritical for companies to claim to care about consumer privacy while

---

148 70 Fed. Reg. 15736 (Mar. 29, 2005) (to be codified at 12 C.F.R. pt. 30, 208, 225, 364, 568, 570).

149 Pub. L. No. 140–191, 110 Stat. 1938 (1996).

150 45 C.F.R. §§ 164.400–164.414 (2020).

151 *Id.* § 164.402.

152 16 C.F.R. §§ 318.1–318.9 (2020).

153 *See id.* § 318.3.

154 15 U.S.C.A. § 57a (West 2020); 16 C.F.R. § 318.7.

155 Julie Brill, *Microsoft Will Honor California's New Privacy Rights Throughout the United States*, MICROSOFT (Nov. 11, 2019), https://blogs.microsoft.com/on-the-issues/2019/11/11/microsoft-california-privacy-rights/.

simultaneously discriminating against Americans based on their place of residence.

Many other companies have previously indicated that they would participate in widespread data privacy protection for consumers, but only once Congress has passed a federal data privacy law.[156] Unless the federal government is willing to recognize the merits of the GDPR and adapt those principles to a national framework, this is not likely to happen anytime soon.[157] As such, while consumers outside California may be able to reap the benefits provided by the CCPA, this is currently only on a company-by-company basis rather than federally mandated. For this and other reasons discussed in the next section, the CCPA may actually end up doing more harm than good in the realm of both consumer rights and business interests.

i. State Action May Do More Harm Than Good

The CCPA is an important step forward in the move toward increased consumer protection in the realm of data privacy.[158] However, the Act is limited in scope and could actually mark the beginning of a more confusing era for enforcing consumer rights. As such, the potential impact of the CCPA on the already-confusing world of American data protection is important to consider in showing the significance of creating a federal framework that puts an American spin on the GDPR.

Though the CCPA has only been in force since January 1, 2020, practical limitations on enforcement already abound.[159] First, state enforcement of the Act will be limited for several months, and even after this "grace period" it is unclear how strictly the Act will be able to be enforced by the Attorney General's office. Second, while businesses have already begun the process of notifying Californian consumers of their rights under the CCPA and implementing measures to ensure compliance with the CCPA as it relates to California

---

156 Cat Zakrzewski & Derek Hawkins, *Tech Executives Voice Support for National Privacy Law*, WASH. POST (Sept. 26, 2018, 11:09 AM), https://www.washingtonpost.com/politics/2018/09/26/tech-executives-voice-support-national-privacy-law/.

157 Tony Romm, *Top Senate Democrats Unveil New Online Privacy Bill, Promising Tough Penalties for Data Abuse*, WASH. POST (Nov. 26, 2019, 7:45 AM), https://www.washingtonpost.com/technology/2019/11/26/top-senate-democrats-unveil-new-online-privacy-bill-promising-tough-penalties-data-abuse/.

158 For example, the CCPA has already revealed that Amazon keeps a record of everything customers do on a Kindle, from the moment a person starts and stops reading to when a person highlights a word. Kari Paul, *"They Know Us Better Than We Know Ourselves": How Amazon Tracked My Last Two Years of Reading*, GUARDIAN (Feb. 3, 2020, 3:01 PM), https://www.theguardian.com/technology/2020/feb/03/amazon-kindle-data-reading-tracking-privacy.

159 *Infra* Section III.C.2.ii.

consumers,[160] actual disclosures in response to CCPA requests have not been handled as efficiently.[161]

Finally, California's legacy as a trailblazer in passing novel laws could very well continue with the CCPA, creating a domino effect across the U.S.[162] This may be one of the clearest ways in which the CCPA could eventually cause more harm than good in the realm of securing consumer data privacy rights. If more states pass laws that mimic—but do not reiterate—California's law, then the U.S. will find itself grappling with the most confusing data privacy regime in the world rather than bringing justice to consumers across the nation.

ii. Practical Limitations of State-Specific Data Privacy Laws

The clearest limitation the CCPA faces is its lack of individual enforcement procedures. Because the Act only creates a right for the State Attorney General to file claims against companies allegedly in violation of consumers' rights, it will likely be difficult for individuals to seek redress on their own. Furthermore, the Attorney General's right to bring an enforcement action under the CCPA only took effect on July 1, 2020.[163] However, at present, current Attorney General Xavier Becerra's office must first send businesses warnings that they might be in violation of the law, allowing them 30 days to fix any issues before fines or lawsuits are contemplated.[164] In the meantime, numerous class actions have already been initiated in California courts,[165] while projections indicate that there will only be about two dozen agents assigned to enforcing the Act—in a state with 40 million people—and California's Supervising Deputy Attorney General on Consumer Protection previosuly indicated she will likely have the capacity to prosecute "just three cases per

---

160 The Author, a California resident, received an abundance of email communications in the weeks leading up to January 1, 2020, notifying her of changes to various companies' Privacy Policies and Consent Preferences options in response to the CCPA's scheduled date of effect.

161 Greg Bensinger, *So Far, Under California's New Privacy Law, Firms Are Disclosing Too Little Data—Or Far Too Much*, WASH. POST (Jan. 21, 2020, 7:44 PM), https://www.washingtonpost.com/technology/2020/01/21/ccpa-transparency/.

162 *Infra* Section III.C.3.iii.

163 *CCPA Fact Sheet*, *supra* note 131.

164 *See* Rachel Lerman, *California Begins Enforcing Digital Privacy Law, Despite Calls for Delay*, WASH. POST (July 1, 2020, 7:00 AM), https://www.washingtonpost.com/technology/2020/07/01/ccpa-enforcement-california/ (additionally highlighting that businesses have already asked for, and been denied, extensions of the CCPA's original six-month "grace period" for compliance in light of the COVID-19 pandemic).

165 *See generally* Alysa Zeltzer Hutnik, Paul A. Rosenthal, Tara Marciano & William Pierotti, *CCPA Litigation Round-Up: Q2 2020*, AD LAW ACCESS (July 17, 2020), https://www.adlawaccess.com/2020/07/articles/ccpa-litigation-round-up-q2-2020/.

year."[166] In the months since July 2020, the Office of the Attorney General has already followed up on claims of potential violations,[167] but it is unclear how many Californians will succeed on claims within the confines of the system.[168]

While some businesses are extending CCPA rights beyond California's borders,[169] other companies run the spectrum from coming up short in what they actually disclose, to overwhelming consumers with too much information.[170] This is an issue that other potential state laws will run into as businesses begin to interpret and test the bounds of privacy and protection laws.

iii. The Dangers of a "Domino Effect"

It is unsurprising that California is the first state to pass such a law. The state contributes to a significant portion of the Ninth Circuit's caseload, and the Ninth Circuit falls on the side of the split championing plaintiffs' rights to sue in data breach cases on the basis of the threat of future harm. Moreover, California has often been a leader in passing novel laws that address modern issues. As a result, the CCPA has the potential to become a model statute for other states seeking to take a firmer stance on the issue of data breaches and the protection of consumer privacy. While this could serve to introduce more measures into the U.S. that mirror the GDPR, this is not necessarily a good thing. Because no two laws can seemingly ever be completely alike, businesses that are already compliant with the GDPR—but are now subject to the CCPA as well—may still find themselves facing additional obligations under California's law. If other states follow California's model and create specific laws limited to their own territories, then the U.S. could end up with multiple data protection frameworks that overlap or—even worse—contradict one another.

---

166 Bensinger, *supra* note 161.

167 *See* Stacey Gray, *Off to the Races for Enforcement of California's Privacy Law*, FUTURE PRIV. F. (July 10, 2020), https://fpf.org/2020/07/10/off-to-the-races-for-enforcement-of-californias-privacy-law/.

168 It is worth noting that the California Privacy Rights Act ("CPRA"), also known as Prop. 24, will appear on the November 3, 2020, ballot. The CPRA seeks to fix several problems remaining in the CCPA and promises short-term consumer benefits, but it has come under scrutiny for the lack of certainty provided on long-term privacy impacts. *See* Maureen Mahoney, *CPRA Promises Short-Term Consumer Benefits, Long-Term Uncertainty*, IAPP (July 22, 2020), https://iapp.org/news/a/cpra-promises-short-term-consumer-benefits-long-term-uncertainty/.

169 *Infra* Section III.C.2.iv.

170 Bensinger, *supra* note 161. For example, Uber and Lyft maintain troves of personal data collected from customers' accounts, but both companies failed to include some of this information in CCPA requests—such as ratings information and customer service calls. *Id.* In the same vein, Amazon has yet to share what data it collects in its camera-equipped convenience stores, according to some requests. Fowler, *supra* note 130. On the other hand, Twitter's initial method for responding to requests was to send users "a file in a JavaScript format that is difficult for non-techies to open." Bensinger, *supra* note 161.

An increased number of nuanced or conflicting state data protection laws that are limited in application will only cause more confusion, especially within the circuits. Such a future may even include two or more "uniform" frameworks, wherein states may attempt to adopt similar laws along circuit "party lines," thus forcing the Federal Government to attempt to stitch together a national law that incorporates all sides but misses the mark altogether.

In order for the U.S. to get ahead of this possible issue, either Congress or the Supreme Court must address the need for a uniform, federal framework before more states inadvertently contribute to the problem by attempting fix it themselves.

iv. Many American Businesses Already Comply with the GDPR

Part II.D explained that the GDPR extends protection to all EU citizens, thereby imposing an obligation on any company whose business "touches" an EU citizen, no matter the company's location.[171] With the rise of globalization in recent decades, more and more U.S.-based entities conduct business in foreign countries on a daily basis.[172] In addition, advancements in technology have only further facilitated the cross-border movement of data between U.S. and foreign entities.[173] As a result, most American entities engaged in transnational data collection and processing have already been updating their data collection policies to bring their businesses into compliance with the GDPR and related international frameworks.[174] In fact, some of these entities have gone one step further—making GDPR-esque data protection and privacy rights available to all of their customers and contacts.[175]

---

[171] *Supra* Section II.D.

[172] *See* Thomas Hout, *Abandoning Globalization Will Only Hurt U.S. Businesses*, HARV. BUS. REV. (Aug. 20, 2020), https://hbr.org/2020/08/abandoning-globalization-will-only-hurt-u-s-businesses (emphasizing American reliance on foreign markets, especially in the technology sector); *see also* Rick Newman, *Why U.S. Companies Aren't So American Anymore*, U.S. NEWS & WORLD REP. (June 30, 2011, 3:58 PM), https://money.usnews.com/money/blogs/flowchart/2011/06/30/why-us-companies-arent-so-american-anymore.

[173] *See Privacy Shield Program Overview*, PRIVACY SHIELD, https://www.privacyshield.gov/Program-Overview (last visited Mar. 20, 2020).

[174] For example, in 2016, American-owned companies, like Twitter, updated their Privacy Policies to include provisions related to the EU–US Privacy Shield Program. *Our Global Operations and Privacy Shield*, TWITTER: PRIVACY POLICY, https://twitter.com/en/privacy (last visited Sept. 6, 2020). Since the GDPR's entry into force, this and other companies' policies have been updated to include provisions specific to EU citizens. *See, e.g.*, *id.*

[175] For example, when Barbri, a well-known business providing educational resources for law students, updated its Privacy Policy and Cookie Policy to reflect the GDPR standards for EU customers, it took the opportunity to make similar changes to improve the rights of all of its

Undoubtedly, it is much easier for a business to comply with one or a few overarching laws or regulations that may be applied to a larger portion of its clientele than to struggle to keep up with a growing body of law that requires more or less specific regulation of a smaller audience. In the overarching quest to simplify all aspects of data privacy, a uniform national framework based on the principles of the GDPR would not only improve the consumer experience across data collection and post-breach remedy, but it would also improve businesses' experiences with compliance by reducing the number of overlapping and conflicting laws in favor of a streamlined and cohesive collection of rules.

IV. CONCLUSION

In this day and age, consumer data is increasingly valuable, and people have a right to know just how much their data is worth to the companies charged with protecting it. But this is not an issue for the states to decide on their own. Consumers deserve a transparent, unified system that does not make them "wait until hackers commit identity theft or credit-card fraud in order to give [them] standing."[176] Businesses deserve something better, too: a uniform system of rules incentivizing respect for consumer rights and protecting company interests. For the U.S., this translates to the development of a federal framework applicable to all its citizens and residents and the companies that interact with them. The right to know, the right to opt-out, and the right to request deletion are fundamental principles championed by the GDPR, which could positively contribute to the regulation and protection of consumer data in the U.S. By generating a general framework of its own, the U.S. could better deter the type of corporate behavior that tends to result in massive data breaches while allowing consumers to exercise more control over their data as a way to try and mitigate the number and consequences of breaches in the future. It is evermore important to recognize that, at the end of the day, "data subjects" are real human beings whose lives instantly change after a data breach, and "data collectors and processors" are groups of human beings who must be held to a higher standard.

*Isabella Anderson**

---

customers. *See Cookie Policy*, BARBRI (May 25, 2018), https://www.barbri.com/cookie-policy/; *Privacy Policy*, BARBRI (May 25, 2018), https://www.barbri.com/privacy-policy/.

176 Remijas v. Neiman Marcus Grp., L.L.C., 794 F.3d 688, 693 (7th Cir. 2015).

* J.D. Candidate, West Virginia University College of Law, 2021; B.A., Political Science, McGill University 2018. Executive Editor, *West Virginia Law Review*. The Author would like to thank her family for listening to her lengthy ramblings about data privacy and their willingness to learn about the GDPR alongside her. She additionally thanks Professor James Friedberg and her colleagues, from the West Virginia Law Review, for their advice and review during the Note-writing process. Finally, the Author would like to thank the College of Law for helping her apply the knowledge gained over the last year to a Dean Acheson Legal Stage position with the European Court of Justice in 2021. Any errors contained herein are the Author's alone.