ADJUDICATE OR LEGISLATE: THE GREAT DATA BREACH STANDING CIRCUIT SPLIT

IOANNIS KOUTSODENDRIS

I. INTRODUCTION

> Our own information . . . is being weaponized against us with military efficiency. Every day, billions of dollars change hands and countless decisions are made on the basis of our likes and dislikes, our friends and families, our relationships and conversations, our wishes and fears, our hopes and dreams. These scraps of data, each one harmless enough on its own, are carefully assembled, synthesized, traded and sold.[1]

Data is fast emerging as among the world's most valuable commodities. "Alphabet . . . , Amazon, Apple, Facebook, and Microsoft . . . are the five most valuable listed firms in the world."[2] Their rise to immense profitability—a combined twenty-five billion dollars in net profit in the first quarter of 2017[3]—traces a twenty-first century explosion in the quantity of data produced worldwide. The rate of data production is growing exponentially, with International Business Machines ("IBM") noting in 2013 that ninety percent of all data then existing had been created in the past two years alone.[4] Causes for this unprecedented increase are myriad, including greater access to the internet in developing nations; rising smartphone penetration (in the U.S. from barely 20% in 2010 to nearly 70% in 2018);[5] the growth in e-payments such as credit cards and mobile wallets (40% of in-person spending in China is now performed through digital wallets such as Alipay and Apple Pay);[6] and widespread adoption of social media platforms such as Facebook, Instagram, Twitter, and Snapchat.

---

[1] Tim Cook, CEO, Apple Inc., Keynote Address at the European Parliament (Oct. 17, 2018) (transcript available at Sarah Salinas & Sam Meredith, *Tim Cook: Personal Data Is Being "Weaponized Against Us with Military Efficiency,"* CNBC (Oct. 24, 2018), https://www.cnbc.com/2018/10/24/apples-tim-cook-warns-silicon-valley-it-would-be-destructive-to-block-strong-privacy-laws.html).

[2] *The World's Most Valuable Resource Is No Longer Oil, but Data*, ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[3] *Id.*

[4] Ralph Jacobson, *2.5 Quintillion Bytes of Data Created Every Day. How Does CPG & Retail Manage It?*, IBM CONSUMER PROD. INDUS. BLOG (Apr. 24, 2013), https://www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does--cpg-retail-manage-it [https://web.archive.org/web/20180731031835/https://www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does-cpg-retail-manage-it].

[5] *Research Peek of the Week: Smartphone Users in the US Expected to Reach Over 270 Million by 2022*, INTERNET INNOVATION ALL. (July 3, 2018), https://internetinnovation.org/general/research-peek-of-the-week-smartphone-users-in-the-us-expected-to-reach-over-270-million-by-2020.

[6] SUKRITI BANSAL ET AL., GLOBAL PAYMENTS 2018: A DYNAMIC INDUSTRY CONTINUES TO BREAK NEW GROUND 7–8 (2018), https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20

The availability of vast quantities of data is a double-edged sword, giving rise to both major benefits and serious threats. As modern life becomes increasingly dependent on electronic services and communications, vast quantities of personal, and often sensitive, data are generated, captured, and stored by corporations and governments in a manner over which the end user has little to no control. It is often impossible to know which entities are hoarding troves of our personal data. And that data can fall into malicious hands, as 148 million Americans learned in September 2017 when Equifax, one of the United States' three largest consumer credit reporting agencies, announced a data breach that exposed the names, addresses, Social Security Numbers ("SSNs"), and driver's license numbers of millions of Americans.[7] Similarly, a 2013 breach of the search giant Yahoo! released the personal data of three billion users[8] while another data breach in 2015 at the Office of Personnel Management compromised the personal and biometric data of over twenty million people.[9] The best evidence indicates that the problem of data breaches is rapidly worsening.[10] 2019 was the worst year ever for data breaches, with both the number of breaches reported and number of records exposed reaching all-time highs.[11]

Figures 1 & 2. Number of breaches reported, and number of records exposed, respectively.[12]

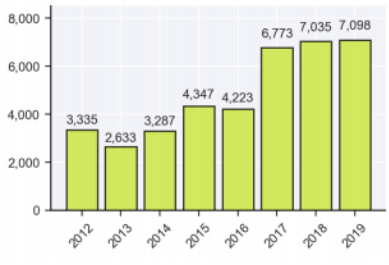

Figure 1: Number of breaches reported each year

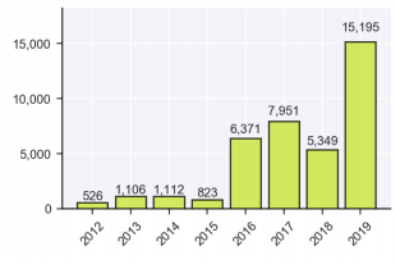

Figure 2: Number of records lost (in millions) each year

Given the immense value of personal data and the increasing zeal with which malicious actors attempt to gain access to it, the United States is in dire need of a robust data privacy regime. So far, however, Congress has not provided a comprehensive legislative solution to address these issues. In fact, the "United States lacks a single, comprehensive federal law that regulates the collection and use of personal information. Instead, the government has approached [data] privacy and security by regulating only certain sectors and types of sensitive information (e.g., health and financial), creating

Services/Our%20Insights/Global%20payments%20Expansive%20growth%20targeted%20opportunities/Global-payments-map-2018.ashx.

[7] *Equifax Data Breach*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/data-breach/equifax/#background (last visited Jan. 22, 2021).

[8] *Id.*

[9] *Id.*

[10] *See id.*

[11] INGA GODDIJN, 2019 YEAR END REPORT: DATA BREACH QUICKVIEW (2020), https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf.

[12] *Id.*

overlapping and contradictory protections."[13] Thus, because the United States lacks a comprehensive data privacy law, it can be difficult for victims of a data breach to understand their legal rights.

The legal rights of data breach victims are an important piece of the data-privacy puzzle. Consumers who have had their data collected and stored, often without their knowledge or consent, should have standing to seek legal redress for their injuries in the event of a breach of their personal information. However, neither the legislature nor the judiciary have provided a workable standard for determining whether a data breach plaintiff has standing to sue in cases involving injuries that have yet to fully mature. Even in cases involving procedural rights granted by statute, the question of standing remains unclear. This uncertainty arises from the injury-in-fact requirement for Article III standing, which sets standards for concreteness and immediacy that an injury must satisfy. The Supreme Court addressed the issues of the concreteness and immediacy with respect to the injury-in-fact requirement in two recent cases: *Clapper v. Amnesty International* and *Spokeo, Inc. v. Robins*.[14] These rulings have resulted in a great deal of confusion in the lower courts in determining which plaintiffs meet the standard for Article III standing in data breach cases, and a high degree of uncertainty for the plaintiffs themselves, even in cases in which Congress has granted a statutory right to sue.

This Note argues that the issue of standing in data breach cases does not exist in a vacuum; rather, it is part of a broader class of gray-area cases in which the Supreme Court looks to Congress for guidance on which harms society has chosen to elevate to the level of a legally cognizable injury. Given the increasingly important role of data in modern life, the rising frequency of data breaches, and the desire of the public to have more control over their personal information, it is incumbent upon Congress to create a comprehensive data privacy regime that recognizes the threat posed by data breaches and the legal right of victims to sue for their injuries. Congress can do this by identifying the types of harms caused by data breaches and establishing procedural rights to vindicate them. The legislature can thereby provide guidance to the courts as to which types of injuries are sufficiently concrete to meet the Article III standards for injury in fact, redressability, and immediacy.

In the alternative, absent a legislative solution from Congress, the judiciary may be in the position to provide a legal solution by resolving a current circuit split on whether a risk of future harm is sufficient to satisfy the injury-in-fact requirement. In order to avoid an over-broad Article III standing, the Supreme Court could issue a limited ruling that allows an

[13] *Id.*; *see* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection (discussing the United States' lack of a single, comprehensive federal law to regulate both the collection and use of consumers' personal information and also providing examples of laws that regulate only specific sectors, like HIPAA).

[14] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 411–15 (2013); Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548–49 (2016). These cases provide support for the proposition that the Supreme Court sometimes uses the injury-in-fact requirement in the context of data privacy cases in order to deny plaintiffs Article III standing. In the case of *Clapper*, the court focused on the "imminence" factor of the injury-in-fact requirement, whereas the *Spokeo* court placed more of an emphasis on "concreteness."

increased risk of future harm from data breaches specifically to satisfy the injury-in-fact requirement. This would resolve a long-standing circuit split and clearly define the rights of parties in data breach cases without over-expanding Article III standing.

Part I of this Note discusses the critical state of affairs regarding data privacy legislation in the United States, a problem exacerbated by the rapid adoption of new technologies and the increasingly important role that electronic data plays in American life. Part II traces a brief history of Article III standing and discusses the injury-in-fact requirement and the Court's modern articulation of the requirement in *Clapper* and *Spokeo*. Parts III and IV discuss the circuit court split on the issue of standing in data privacy cases. Part V calls on the Supreme Court to act by either giving greater deference to Congress on the issue of standing in data breach cases, or by resolving the circuit split to allow an increased risk of future harm to satisfy the injury-in-fact requirement in these cases. Finally, Part VI outlines a potential legislative solution to data breach injuries and urges Congress to clearly define the rights of data breach victims.

II. DATA PRIVACY LEGISLATION IN THE U.S.

A. DISJOINTED CONGRESSIONAL EFFORTS

The United States' approach to data protection legislation is fragmented and reactionary, and the United States has no principal data protection law at the federal level.[15] Instead of one comprehensive data privacy law, data protection legislation in the United States is largely sector-specific, or focuses on particular types of data.[16] This approach has created overlapping, and sometimes contradictory, protections.[17] Some examples of sector-specific legislation passed by Congress include the following:

- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which is the United States' "primary health privacy and security law."[18]
- The Fair Credit Reporting Act of 1970 ("FCRA"), which promotes the accuracy and privacy of consumer information in credit reporting agency files.[19]

[15] *See* STEVEN CHABINSKY & F. PAUL PITTMAN, USA: DATA PROTECTION LAWS AND REGULATIONS 2020 (2020), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (explaining that there is no single principal data protection legislation in the US; instead many different state and federal laws come together to protect the personal data of Americans).

[16] *Id.* (citing to the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 *et seq.*; Children's Online Privacy Protection Act, 15 U.S.C. § 6501; Video Privacy Protection Act, 18 U.S.C. § 2710 *et seq.*; and Cable Communications Policy Act of 1984, 47 U.S.C. § 551 as examples of legislation that target specific sectors).

[17] O'Connor, supra note 13 (explaining that state and federal laws often conflict with each other and can have incompatible provisions and varying requirements).

[18] See Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996); O'Connor, supra note 13.

[19] *See* Fair Credit and Reporting Act of 1970, 15 U.S.C. § 1681.

- The Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), which amended the FCRA to provide additional identity theft protections and bolster credit transaction security.[20]

An issue with having separate statutes for different sectors or types of data is that there is no standard procedure for how corporate entities are supposed to respond in the event of a data breach. This is because the necessary response varies depending on the type of data compromised. For example, while some federal laws like HIPAA have a breach notification rule, which "requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information,"[21] statutes protecting other types of data lack similar protections. In several cases, this has led states to take data privacy matters into their own hands by passing their own data breach notification laws, like California's Civil Code section 1798.82 and New York's General Business Law section 899-aa. The California law requires businesses to "disclose a breach . . . in the security of the data to a resident of California . . . whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person,"[22] while the New York law has similar requirements.[23]

B. STATES COMING TO THE RESCUE?

The passage of breach-notification laws by individual states is likely to lead to a fragmented, confusing legislative scheme for consumers and corporations alike. Moreover, state data privacy laws often lack sufficient penalties to redress victims' injuries, or result in the adoption of greater security measures. The punitive effect of these laws has largely been limited to publicly "shaming" companies that do not disclose breaches with small monetary fines.[24] This public shaming provides little beyond a public relations incentive to advance the adoption of stricter security measures, and victims are often left to bear the burden of their injuries by "maintain[ing] ongoing vigilance about identity theft and other fraud, some of which could occur years after the initial incident."[25] As it stands, "[m]ost data breaches . . . do not result in significant financial harm to companies[,] [and] [e]ven when regulators such as the [Federal Trade Commission ("FTC")] get involved, the likelihood of any monetary fine is small."[26] Thus, although state solutions to data privacy issues are a welcome start, the passage of a comprehensive federal data privacy statute is necessary to simplify things

[20] *See* Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1953 (2003).

[21] *Breach Notification Rule*, U.S. DEP'T OF HEALTH AND HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Jan. 22, 2021) (providing an example of a federal law which currently has a data breach notification requirement).

[22] CAL. CIV. CODE § 1798.82 (Deering 2021).

[23] *See* N.Y. GEN. BUS. LAW § 899 (Consol. 2019).

[24] O'Connor, *supra* note 13.

[25] *Id.* (arguing that data breach notification laws alone will do little to actually result in meaningful improvements in data security practices, and that clear rules are needed to incentivize companies to secure data).

[26] *Id.*

for consumers, and to incentivize businesses to better protect consumer data. Finally, given the less-sophisticated nature of consumers, such a law would require a mechanism by which victims can mitigate burden-shifting so that consumers are not left to bear the costs of a company's mismanagement of their data.[27]

The nature of electronic data necessitates a centralized solution to the issue of data privacy, and individual state solutions would create confusion for businesses. Companies doing business in several states would have great difficulty assessing their liabilities because they may have to comply with several different standards, thereby raising costs. Similarly, consumers would face difficulty in understanding their rights if they regularly travel to other states where protections may be different than those in their home states. Moreover, the implementation of individual state laws risks the creation of pro-corporation or pro-consumer havens where companies may be reluctant to do business, or consumers may travel in order to enjoy greater protections.

Congress, as opposed to the states themselves, is uniquely positioned to provide a solution to victims in data breach cases because it can create a comprehensive solution that applies uniformly across all states. Perhaps more importantly, the Supreme Court has stated that "Congress can build on common law conceptions of injury . . . to 'identify intangible harms that meet minimum Article III requirements' and establish new causes of action to remedy such harms."[28] Thus, Congress may be best suited to solve a critical piece of the data-privacy puzzle by elevating intangible data breach injuries to concrete status, and by establishing private rights of action that would allow for victims to vindicate harms that would otherwise not have satisfied the requirements for standing.

C. THE EUROPEAN MODEL: THE GDPR

The European Union's ("EU") recently enacted General Data Protection Regulation ("GDPR") provides a helpful model for what a comprehensive American data privacy law might look like. The GDPR is a wide-reaching law that applies to companies that offer goods or services to, or process the personal data of, EU citizens and residents.[29] Unlike the previously-discussed California and New York breach notification laws, the GDPR levies stiff penalties for violations: maximum fines under the law can reach twenty million Euros or four percent of global revenue, and data subjects have a private right to compensation for damages as well.[30] In the case of a data breach specifically, the GDPR gives companies a uniform seventy-two-hour period to notify the subject of the breach before a penalty is levied.[31] The GDPR protections are not merely retrospective; instead, many of the

[27] *See id.*

[28] Wilson C. Freeman & Kevin M. Lewis, Cong. Rsch. Serv., R45636, Congressional Participation in Litigation: Article III and Legislative Standing 3 (2019), https://fas.org/sgp/crs/misc/R45636.pdf (illustrating the willingness of the Supreme Court to recognize Congress's establishment of new causes of action where none before had existed).

[29] *What Is GDPR, the EU's New Data Protection Law?*, GDPR, https://gdpr.eu/what-is-gdpr (last visited Jan. 22, 2021) (providing background information on the General Data Protection Regulation).

[30] *Id.*

[31] *Id.*

law's protections are aimed at securing the sources of data privacy issues. For example, the GDPR sets uniform standards for obtaining the consent of consumers and for handling their data, including a requirement to implement "appropriate technical and organizational measures" to protect data, such as two-factor authentication and end-to-end encryption.[32]

The effects of the GDPR on Europe's data privacy regime have already been felt. The law firm DLA Piper reported that as of January 2020, over 160,000 data breach notifications have been issued across the EU since the introduction of the law.[33] Moreover, the law's punitive measures are bringing data privacy issues into the global spotlight. For example, European data protection regulators have imposed €114 million in fines under the law, and DLA Piper partner Ross McKean commented, "[The] GDPR has driven the issue of data breach well and truly into the open. The rate of breach notification has increased by over 12% compared to last year's report and regulators have been busy road-testing their new powers to sanction and fine organisations."[34] If nothing else, the GDPR has raised awareness for data privacy and penalized companies that did not sufficiently protect consumer data from attack. Thus, the European law may serve as a model for a comprehensive American approach to data privacy legislation.

D. ALTERNATIVES TO COMPREHENSIVE DATA PRIVACY LEGISLATION

Absent the creation of a comprehensive data privacy regime by the legislature, Congress can resolve many data privacy disputes by elevating some intangible injuries to concrete status.[35] Additionally, the judiciary could provide stop-gap protections using existing statutes by granting standing to data breach plaintiffs that have suffered intangible injuries. By giving data breach victims a procedural right to sue in many cases, Congress can send a clear signal to the judiciary that it wishes to elevate certain intangible injuries to concrete status, thus giving consumers an avenue to redress their injuries and guidance to the courts on how to resolve the current circuit split. Moreover, granting consumers procedural rights to sue would serve as a deterrent to companies which currently have lax data privacy policies. This may induce corporations to adopt better data protection standards even in the absence of a more comprehensive piece of legislation, such as the GDPR. The legal feasibility of such an approach, however, is a matter of constitutional law and will be discussed in the sections that follow.

---

[32] *Id.* Organizational measures include things like staff training, adding data privacy policies to employee handbooks, and limiting access to personal data to only employees that need access to such data.

[33] *EUR114 Million in Fines Have Been Imposed by European Authorities Under GDPR*, DLA PIPER (Jan. 20, 2020), https://www.dlapiper.com/en/global/news/2020/01/114-million-in-fines-have-been-imposed-by-european-authorities-under-gdpr. Ross McKean, a DLA partner, also noted that the amount of fines imposed to date "is relatively low compared to the potential maximum fines that can be imposed under GDPR, indicating that [it is] still in the early days of enforcement . . . [and] regulators [will] ramp up their enforcement activity." *Id.*

[34] *Id.*

[35] *See generally* Stephen P. Mulligan et al., Cong. Rsch. Serv., R45631, Data Protection Law: An Overview (2019), https://fas.org/sgp/crs/misc/R45631.pdf.

III. AN ALTERNATE APPROACH: THE LEGAL BACKGROUND OF ARTICLE III STANDING

A. CONSTITUTIONAL ORIGINS AND THE *LUJAN* TEST

Article III, Section 2 of the Constitution "limits the exercise of the federal courts' judicial power to . . . 'Cases' and 'Controversies.'"[36] In its landmark 1992 decision *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992), the Supreme Court articulated a three-part test for this "standing" to reach federal court.[37] To gain standing, a plaintiff must have suffered an "injury in fact" that constitutes an "invasion of a legally protected interest which is (a) concrete and particularized . . . and (b) 'actual or imminent, not "conjectural" or "hypothetical."'"[38] There must also be a "causal connection between the injury and the conduct complained of," such that the injury is "fairly . . . trace[able] to the challenged action of the defendant."[39] Finally, it must be "likely" that a favorable decision would redress the injury suffered, and the party seeking federal jurisdiction bears the burden of proving the above elements.[40]

The above test implies a "floor" for the conferral of Article III standing because a plaintiff must prove an injury in fact, causation, and redressability to have their case heard. Throughout the evolution of the standing doctrine, the Court has not hesitated to acknowledge the existence of such a floor. For example, in 1979, the Court in *Gladstone, Realtors v. Bellwood*, 441 U.S. 91 (1979), stated, "In no event . . . may Congress abrogate the Art. III minima."[41] However on several occasions, the Court has conceded its willingness to relax the requirements for standing in contexts involving procedural rights.[42] As the *Lujan* Court explained, "There is this much truth to the assertion that 'procedural rights' are special: The person who has been accorded a procedural right to protect his concrete interests can assert that right without meeting all the normal standards for redressability and immediacy."[43] Thus, in *Lujan*, the Court expressed its willingness to deviate from the majority's standing test in some cases to bestow Article III standing

[36] U.S. CONST. art. III, § 2, cl. 1; FREEMAN & LEWIS, *supra* note 28, at 2 (citation omitted).
[37] *See* Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992).
[38] *Id.* at 560.
[39] *Id.*
[40] *Id.* at 561. The likelihood of redressability is measured against whether it would be "speculative" that the injury will be redressed by a favorable decision.
[41] Gladstone Realtors v. Bellwood, 441 U.S. 91, 100 (1979) (circumscribing the ability of Congress to give standing to plaintiffs in cases where the requirements of Article III are not met). Preceding this, however, the Court stated that "Congress may, by legislation, expand standing to the full extent permitted by Art. III, thus permitting litigation by one 'who otherwise would be barred by prudential standing rules.'" *Id.*
[42] Evan Tsen Lee & Josephine Mason Ellis, *The Standing Doctrine's Dirty Little Secret*, 107 NW. U. L. REV. 169, 174 (2012) (arguing that the Supreme Court's decision in *Massachusetts v. EPA* and Justice Kennedy's footnote in *Lujan* are proof of the acknowledgement that the causation and redressability requirements of Article III standing are sometimes optional).
[43] *Lujan*, 504 U.S. at 589, n.7 (Scalia further provides an application of the principle that procedural rights get special treatment, stating: "Thus, under our case law, one living adjacent to the site for proposed construction of a federally licensed dam has standing to challenge the licensing agency's failure to prepare an environmental impact statement, even though he cannot establish with any certainty that the statement will cause the license to be withheld or altered, and even though the dam will not be completed for many years.").

upon plaintiffs to whom Congress has granted a procedural right to bring suit.[44]

The Court's subsequent *Massachusetts v. Environmental Protection Agency* ("EPA"), 549 U.S. 497 (2007) decision further exemplified its willingness to deviate from the Article III requirements in certain cases. The Court in *Massachusetts v. EPA* found that "Massachusetts had standing to seek judicial review of the [EPA]'s denial of [plaintiff's] petition to regulate greenhouse gases [where] [t]he State's injury-in-fact was the potential loss of its coastal lands to rising sea levels."[45] Expressing the principle that Congress may accord procedural rights that will be subject to relaxed redressability and imminence standards, the Court wrote

> [A] litigant to whom Congress has "accorded a procedural right to protect his concrete interests . . . can assert that right without meeting all the normal standards for redressability and immediacy." When a litigant is vested with a procedural right, that litigant has standing if there is some possibility that the requested relief will prompt the injury-causing party to reconsider the decision that allegedly harmed the litigant.[46]

The Court conceded that "some possibility" that state coastal lands would be lost absent the regulation sought was sufficient to support standing where Congress had granted a procedural right to sue.[47] In the context of challenging an agency action wrongfully withheld, the Court reasoned that the procedural right freed the state from meeting the normal imminence standard, and thus, "Massachusetts did not have to meet the normal imminence standard . . . [i]t merely needed to show that there was 'some possibility' that such regulation would somewhat diminish the risk that coastal lands would be lost."[48]

B. PROCEDURAL RIGHTS IN INFORMATIONAL INJURY CASES

The Supreme Court has consistently awarded standing to plaintiffs in "informational injury" cases in which plaintiffs have been granted a procedural right by Congress, suggesting that there are "two different levels of the standing doctrine—one for traditional common law review . . . and another for cases in which Congress has granted a procedural right to review."[49] For example, the private right of action created by the Freedom of Information Act ("FOIA"), which provides the public the right to request

---

[44] *See id.*

[45] Lee & Ellis, *supra* note 42, at 192 (arguing that "intellectual honesty" caused Justice Antonin Scalia to note in the *Massachusetts vs. EPA* decision that federal courts have long tolerated similar suits that "concededly do not meet Article III requirements for redressability and imminence.").

[46] Massachusetts v. EPA, 549 U.S. 497, 517–18 (2007) (illustrating the principle that, while the ruling in *Massachusetts v. EPA* may seem like an outlier, it appears to be part of a broader class of gray-area cases where federal courts have been willing to relax the Article III standing requirements in cases involving procedural rights created by Congress).

[47] Lee & Ellis, *supra* note 42, at 193 (arguing that *Lujan* and *Massachusetts v. EPA* were potentially the first instances where the Supreme Court "admitted" that the standing requirements may be relaxed).

[48] *Id.*

[49] Lee & Ellis, *supra* note 42, at 199.

records access from any federal agency,[50] rests on standing requirements relaxed similarly to those in *Massachusetts v. EPA*. Contrary to the analysis in a standard case, the procedural right created by FOIA means that "anyone whose request for specific information [pursuant to FOIA] has been denied has standing to bring an action; the requester's circumstances—why he wants the information, what he plans to do with it, what harm he suffered from the failure to disclose—are irrelevant to his standing."[51] Therefore, plaintiffs in FOIA actions who ostensibly have suffered no injury outside of a denial of their procedural right to information granted by Congress will be awarded standing to sue under *Zivotofsky* ex rel. *Ari Z. v. Secretary of State*.

Severe relaxation of the injury-in-fact requirement is not just limited to FOIA cases and has extended to other informational injury cases, as well. For example, in *Federal Election Commission* ("FEC") *v. Atkins*, 524 U.S. 11 (1998), a group of voters filed suit under the Federal Election Campaign Act of 1971 ("FECA") to challenge the decision by the FEC to not classify the American Israel Public Affairs Committee as a "political committee" that would subject it to certain reporting requirements, such as disclosing its political contributions—information that plaintiffs sought.[52] The Court noted that "[t]he injury of which respondents complain—their failure to obtain relevant information—is an injury of a kind that FECA seeks to address."[53] Essentially, the Court recognized that the plaintiffs' injury in fact was the invasion of a procedural right granted by Congress under FECA. FOIA and FECA present just two examples of a broader class of cases in which the Court has shown its willingness to deviate from the usual standing requirements when Congress has granted plaintiffs a procedural right to sue. Thus, Congress's grant of a procedural right to data breach plaintiffs would allow the Court to use similarly relaxed standing requirements in data breach cases.

IV. INCONSISTENCY: THE EVOLUTION OF A CIRCUIT COURT SPLIT

A. *CLAPPER V. AMNESTY INTERNATIONAL USA*

As consumers have sought redress for privacy-related injuries, and in the absence of congressional intervention, the Supreme Court has revisited the issue of Article III standing in two privacy-related cases: *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), and *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). In these rulings, the Court has caused further confusion as to what injuries are sufficient to confer Article III standing in data breach cases, particularly with respect to what the rights and liabilities of parties in data breach cases are and the injury-in-fact requirement in cases in which there is an increased risk of future harm.

---

[50] *What is the FOIA?*, FOIA.GOV, https://www.foia.gov/faq.html (last visited Mar. 4, 2021).

[51] Zivotofsky *ex rel.* Ari Z. v. Sec'y of State, 444 F.3d 614, 617 (D.C. Cir. 2006) (citing Warth v. Seldin, 442 U.S. 490, 514 (1975), in support of the proposition that "Congress may create a statutory right or entitlement the alleged deprivation of which can confer standing to sue even where the plaintiff would have suffered no judicially cognizable injury in absence of the statute.").

[52] Lee & Ellis, *supra* note 42, at 198.

[53] FEC v. Akins, 524 U.S. 11, 20 (1998).

In *Clapper*, plaintiffs challenged the constitutionality of section 702 of the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. § 1881a.[54] To establish standing, the plaintiffs alleged that the sensitive nature of their work (which involved communication with individuals who were likely the target of surveillance under § 1881a) required them to "take costly and burdensome measures to protect the confidentiality of their international communications."[55] The Court disagreed. Instead, the Court ruled that plaintiffs lacked standing because a "threatened injury must be certainly impending to constitute injury in fact" and "allegations of possible future injury are not sufficient."[56] Further, the Court rejected the plaintiffs' fears of communication interception as "highly speculative" because they relied on a "highly attenuated chain of possibilities" that could not be considered "certainly impending."[57] As to the remedial measures the plaintiffs had taken, the *Clapper* Court rejected them as the basis for standing: "[A plaintiff] cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[58] Like the measures used by the plaintiffs in *Clapper*, the protective measures employed by consumers, which often include credit monitoring and ordering new forms of identification, can be costly and burdensome. Therefore, the *Clapper* ruling is problematic in the context of data breach harms, which, by their nature, might require victims to take prophylactic measure immediately after they learn their data has been compromised—actions that courts may not consider sufficient in their own right to constitute an injury in fact.

B. THE NATURE OF DATA BREACH HARMS

Clapper greatly weakened plaintiffs' positions in the context of data breach litigation because data breach victims were tasked with the likely insurmountable proposition of providing facts sufficient to show that their injuries are certainly impending. *Clapper* armed defendants with the ability to present plaintiffs' claims as "depending on a series of speculative or hypothetical possibilities that are not certain to occur," thus making it likely that cases of this nature would be thrown out for lack of standing.[59] Data breach plaintiffs under a "certainly impending" standard bear the impossible burden of proving that the actions of a third party, such as an identity thief, are nearly certain to occur in the future. It is possible that a victim's information will never be used in an injurious way. However, the occurrence of a breach not only puts victims in apprehension of future injuries, but

[54] 50 U.S.C. § 1881a. This statute allows the Attorney General and the Director of National Intelligence to authorize surveillance of non-U.S. persons located outside of the United States after seeking the approval of the Foreign Intelligence Surveillance Court.

[55] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402 (2013).

[56] *Id.* at 409 (emphasis removed) (citation omitted).

[57] *Id.* at 410.

[58] *Id.* at 416. This was in reference to plaintiff's taking of "costly and burdensome measures to protect the confidentiality of their communications." *Id.* at 402. The Court rejected plaintiff's argument in this regard.

[59] Edward P. Boyle et al., The Impact of the Supreme Court's Recent Decision in Clapper v. Amnesty International USA on Privacy and Data-Security Litigation, VENABLE LLP (Mar. 2013), https://www.venable.com/insights/publications/2013/03/the-impact-of-the-supreme-courts-recent-decision-i.

breaches of personal data cause concrete and particular injuries in the form of remedial measures taken to secure that data.

This speaks to the main flaw in the application of the certainly impending standard to data breach litigation: it fails to recognize the often-latent nature of injuries in data breaches. The harms resulting from a data breach may not manifest until a significant period of time has passed. "The data is sold off, and it could be a while before it's used . . . [and] [t]here's often a very big delay before having a loss."[60] In effect, this makes injuries from data breaches more analogous to the latent injuries identified in the asbestos cases of the late twentieth century, in which impairment "often would not occur for decades."[61] The issue with applying the certainly impending standard to data breach harms is that, much like with asbestos exposure, the causal chain leading to a plaintiff's harm has already been set into motion long before the final injury has fully manifested. And once the injury from a data breach manifests, the harm can be profound.

The nature and extent of a data breach injury can depend on a number of factors, including the type and quantity of information compromised and the identity of the unauthorized third party who accessed the information. For example, if an individual's financial information is compromised, identity thieves may "plunder victims' credit," incurring fraudulent debts that harm victims' credit scores and, in some cases, cause victims to file for bankruptcy protection.[62] The effects of a data breach on individuals can be even more far-reaching. Because of the importance of credit scores in consumer finance, a data breach victim whose personal financial information has been compromised may be denied approval for loans, be ineligible for lower interest rates on short-term borrowing like credit cards, or risk losing their homes altogether.[63]

Another issue in remediating identity theft is the difficulty and cost of changing some types of personal information. On average, the cost of repairing identity theft is $1,769 and up to thirty hours to resolve issues when unauthorized accounts are opened in victims' names.[64] Some personally identifying information, like SSNs, are highly burdensome to change. SSNs, which are often targeted in data thefts, are typically assigned at birth and are used as an identifier in many sensitive transactions, such as obtaining credit, getting a passport, or receiving certain government benefits. But changing one's SSN is a time-consuming process, requiring the completion of an in-person application at a Social Security office, providing "a statement explaining the reasons for needing a new number," providing "current, credible, third-party evidence documenting the reasons for needing a new number," and producing original documents establishing the applicant's

[60] Andrea Peterson, *Data Exposed in Breaches Can Follow People Forever. The Protections Offered in Their Wake Don't.*, WASH. POST (June 15, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/06/15/data-exposed-in-breaches-can-follow-people-forever-the-protections-offered-in-their-wake-dont.

[61] Paul D. Carrington, Asbestos Lessons: The Consequences of Asbestos Litigation, 26 REV. LITIG. 583, 587 (2007).

[62] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 757 (2018).

[63] *Id.*

[64] *Id.*

citizenship status, age, and identity.[65] The potential harms presented by data breaches are clearly significant. Therefore, it is reasonable to expect the victims of data breaches to take preemptive steps to protect their data once it has been compromised. Thus, application of the certainly impending standard from *Clapper* fails to recognize the latent nature of data breach injuries and places the burden on plaintiffs to bear the costs of reasonable actions taken in response to the mishandling of their data.

C. *SPOKEO, INC. V. ROBINS*

The Supreme Court revisited the injury-in-fact requirement for Article III standing in 2016 with its ruling in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). In *Spokeo*, the plaintiff alleged a violation of the FCRA, a law that Congress passed in 1970 with the "stated intent of 'prevent[ing] consumers from being unjustly damaged because of inaccurate or arbitrary information in a credit report.'"[66] In order to achieve that aim, the FCRA established a number of requirements that consumer reporting agencies must follow concerning the creation and use of consumer reports, including language which requires agencies to "follow reasonable procedures to assure [the] maximum possible accuracy of [their reports]."[67] The FCRA also provided that "any person who willfully fails to comply with any requirement . . . with respect to any consumer is liable [to that person]" for actual damages or statutory damages of $100 to $1,000 for each violation.[68]

Spokeo, Inc. runs a "people search engine," which accepts the input of a person's name, phone number, or e-mail address and returns results about the subject of the search.[69] Spokeo performed one of these searches on Robins, but some of the information it collected and then disseminated about him was factually incorrect.[70] Robins filed suit once he became aware of the inaccurate profile, alleging that Spokeo had willfully violated the FCRA by incorrectly stating that he was an employed, affluent man in his fifties with children—none of which was true.[71] Robins's alleged injury was that Spokeo's violation of the FCRA negatively affected his employment prospects.[72]

In issuing its decision, the Supreme Court vacated and remanded to the Ninth Circuit, stating that although the lower court had properly established that Robins's injury was particularized, it failed to consider the concomitant requirement that an injury in fact also be concrete.[73] Instead, the Ninth Circuit had erroneously concluded that Robins's injuries were "concrete, *de*

---

[65] *See Can I Change My Social Security Number?*, SOC. SEC. ADMIN. (Nov. 29, 2019), https://faq.ssa.gov/en-US/Topic/article/KA-02220.

[66] Recent Cases: Standing – Class Actions – Ninth Circuit Allows Fair Credit Reporting Act Class Action to Proceed Past Standing Challenge. – Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. 2017), 131 HARV. L. REV. 894, 894 (2018).

[67] 15 U.S.C. § 1681e(b).

[68] 15 U.S.C. § 1681n(a)(1)(A).

[69] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1544 (2016).

[70] *Id.*

[71] Recent Cases: Standing – Class Actions – Ninth Circuit Allows Fair Credit Reporting Act Class Action to Proceed Past Standing Challenge. – Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. 2017), supra note 66, at 895.

[72] *Id.*

[73] *See Spokeo*, 136 S. Ct. at 1548.

facto" injuries.[74] The Ninth Circuit came to that conclusion because Robins alleged that Spokeo "violated *his* statutory rights," and "Robins's personal interests in the handling of his credit information are *individualized rather than collective*."[75] The Court agreed with the Ninth Circuit that a "concrete" injury must be "*de facto*," meaning that "it must actually exist."[76] However, the Court further elaborated on concreteness, stating that a "concrete" injury is not necessarily synonymous with a "tangible" harm; rather, intangible harms could constitute an injury in fact if "both history and the judgment of Congress" so indicate.[77] Moreover, the Court particularly stressed the importance of Congress's judgment and instruction, noting that "Congress is well positioned to identify intangible harms that meet minimum Article III requirements," and pointing to its decision in *Lujan* which recognized the legislature's power to "define injuries . . . that will give rise to a case or controversy where none existed before."[78]

The preceding analyses appear to give Congress *carte blanche* to decide what constitutes an injury in fact. However, the Court then circumscribed Congress's power to identify and elevate intangible harms, stating that its role in doing so "does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[79] Instead, Article III standing still requires a concrete injury "even in the context of a statutory violation," and allegations of a bare procedural violation divorced from any concrete harm do not normally satisfy the injury-in-fact requirement of Article III.[80]

The *Spokeo* Court did not completely shut the door on the possibility of procedural violations alone being sufficient for Article III standing. The decision noted that a risk of real harm can satisfy the concreteness requirement: the violation of a statutorily-granted procedural right "*can be sufficient* in some circumstances to constitute injury in fact," and a plaintiff in such cases "need not allege any *additional* harm beyond the one Congress has identified."[81] This somewhat paradoxical about-face has understandably led to a split among the circuit courts in determining which types of injuries are sufficiently concrete for the conferral of Article III standing in data breach cases, in which the violation of a procedural right in some cases will be sufficient for standing, and in others will not.

[74] *Id.*
[75] *Id.* (original emphasis) (citation omitted).
[76] *Id.*
[77] *Id.* at 1549.
[78] *Id.* (original emphasis) (citation omitted).
[79] *Id.*
[80] *See id.*
[81] *Id.* (first emphasis added).

V. THE DATA BREACH CIRCUIT SPLIT

A. DIVERGENT STANDARDS

A number of federal circuit courts have issued conflicting rulings with respect to standing in data breach cases in the wake of *Spokeo*. In the Sixth, Seventh, Ninth, and D.C. Circuits, the lone fact that a data breach has occurred has typically been sufficient to confer Article III standing.[82] These circuits have concluded "that the heightened risk of identity theft [is] enough to clear the 'low bar' for establishing standing at the pleading stage."[83] On the other hand, the Second, Third, Fourth, and Eighth Circuits utilize a standard that requires proof of more concrete harm.[84] Specifically, these circuits have held that some sort of concrete financial harm is required to confer standing in a data breach case.[85]

B. THE SIXTH, SEVENTH, NINTH, AND D.C. CIRCUITS

The federal circuit courts have adopted disparate standards thus far to address the issue of standing in data breach cases as part of what is an ever-widening circuit split. The Sixth, Seventh, Ninth, and D.C. Circuits have adopted a pro-consumer position on standing in data breach cases that utilizes an "increased risk of future harm" standard, in which a plaintiff's increased risk of future harm from a data breach "may be sufficient to confer standing to sue even in the absence of specific subsequent harm to the consumer."[86]

1. The Pro-Consumer View: *Ree v. Zappos.com, Inc.*

One recent example of an application of this standard is the Ninth Circuit's decision in *Ree v. Zappos.com, Inc.*, 888 F.3d 1020 (2018). In *Zappos*, hackers breached the servers of the online retailer Zappos, Inc. and allegedly stole the "names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information of more than [twenty-four] million Zappos customers."[87] While plaintiffs in other cases stemming from this incident had alleged that the hackers used their stolen information to conduct fraudulent financial transactions, the plaintiffs' appeal in *Zappos* focused on claims "based on the hacking incident itself, not any subsequent illegal activity."[88] The court held that a plaintiff's allegation of "a credible threat of real and immediate harm" stemming from the theft of their personal data is sufficient to satisfy the injury-in-fact requirement of Article III standing.[89] Specifically, the court

[82] Amanda Lawrence et al., *The Great Data Breach Standing Circuit Split*, LAW360 (Jan. 25, 2019, 3:29 PM), https://www.law360.com/articles/1121370/the-great-data-breach-standing-circuit-split.

[83] Allison Grande, *DC Circ. Piles onto Standing Split with Data Breach Ruling*, LAW360 (June 28, 2019, 5:32 PM), https://www.law360.com/articles/1173454/dc-circ-piles-onto-standing-split-with-data-breach-ruling.

[84] Lawrence et al., *supra* note 82.

[85] *Id.*

[86] *Id.*

[87] *In re* Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018).

[88] *Id.*

[89] *See id.*

noted that plaintiffs' allegations that the type of information accessed in the Zappos breach, such as credit card numbers and e-mail addresses, could be used to commit identity theft were sufficient to constitute an injury in fact partly because "Congress has treated credit card numbers as sufficiently sensitive to warrant legislation . . . to reduce the risk of identity theft."[90] The court reasoned that it was highly likely that plaintiffs who had not yet been harmed would suffer identity fraud as a result of the breach, pointing to the second class of plaintiffs who had already suffered financial losses and "alleged that the hackers had already commandeered their accounts or identities using information taken from Zappos."[91]

2. Reconciliation: *Clapper*, *Krottner*, and the Injury-In-Fact Requirement

To arrive at this ruling, the Ninth Circuit had to revisit a standard established by *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), a case in which the court had previously held that plaintiffs' allegations of a credible threat of real and immediate harm are sufficient for Article III standing in the context of data-theft litigation.[92] However, in order to apply the ruling in *Krottner* to *Zappos*, the court had to address whether the Supreme Court's *Clapper* decision was irreconcilable with the reasoning in *Krottner*.

In *Krottner*, a thief stole a laptop that contained the sensitive information of approximately ninety-seven thousand Starbucks employees; Starbucks subsequently notified the affected employees and some employees sued, with their only allegation being an "increased risk of future identity theft."[93] Ultimately, the court in *Krottner* determined that a credible threat of real and immediate harm was sufficient to satisfy the injury-in-fact requirement for Article III standing.[94] However, this ruling became problematic in light of the ruling in *Clapper* because the *Clapper* Court rejected the idea that a risk of future harm could serve as the basis for standing. Instead, the *Clapper* Court determined that "an objectively reasonable likelihood" of injury alone was inconsistent with the requirement that "threatened injury must be certainly impending to constitute injury in fact."[95]

The court in *Zappos* determined that the rulings in *Krottner* and *Clapper* were reconcilable. This is because, unlike the chain of inferences required to collect the plaintiffs' communications in *Clapper*, injury to the plaintiff in *Krottner* "did not require a speculative multi-link chain of inferences" because the stolen laptop had all of the information on it necessary to commit identity theft.[96] Moreover, *Clapper*'s standing analysis was "especially rigorous" because the case involved a sensitive national security context and foreign affairs.[97] Finally, the court recognized that the Supreme Court has

[90] *See id.* at 1027–28. The legislation enacted by Congress and referenced in the text is 15 U.S.C. § 1681c(g), or FACTA, which provides for the truncation of credit card and debit card numbers to protect them from theft.
[91] *See id.*
[92] Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010).
[93] *In re Zappos*, 888 F.3d at 1025.
[94] *See Krottner*, 628 F.3d at 1143.
[95] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013) (citation omitted).
[96] *In re Zappos*, 888 F.3d at 1026.
[97] *Clapper*, 568 U.S. at 408.

acknowledged the injury-in-fact requirement may be satisfied by an injury "certainly impending," or by a "substantial risk" of injury.[98]

Thus, the Ninth Circuit determined that the Supreme Court's ruling in *Clapper* was reconcilable with their ruling in *Krottner*, and that it controlled the result in *Zappos*. This decision is noteworthy because it reaffirmed the Ninth Circuit's adherence to the view that a credible threat of real and immediate harm will constitute an injury in fact. Moreover, *Zappos* further widened the gulf between circuits that subscribe to a more consumer-friendly view of standing in data-theft cases, and the more stringent standing requirements imposed by opposing circuits. Finally, *Zappos* is significant to data breach rulings because it acknowledges that data breach injuries, which may not conform to typical conceptions of legally cognizable injuries, may deserve redress "even if they pose a risk of injury that is markedly different from the types of cases that typically find their way into federal court."[99]

C. THE SECOND, THIRD, FOURTH, AND EIGHTH CIRCUITS

On the other side of the circuit split, the Second, Third, Fourth, and Eighth circuits have held that an increased risk of future harm is insufficient to confer standing in a data breach case; instead, these courts have typically held that some sort of concrete financial harm is required.[100]

1. The Alternate View: *Kamal v. J. Crew Group, Inc.*

A recent illustration of the less consumer-friendly side of the circuit split is the Third Circuit's decision in *Kamal v. J. Crew Group, Inc.*, 918 F.3d 102 (3d Cir. 2019). In *Kamal*, the Third Circuit held that a plaintiff's action alleging a FACTA violation "from a store's printing of both the first six and last four digits of his credit card number on his receipts in violation of 15 U.S.C.S. § 1681c(g)" was "properly dismissed . . . for lack of . . . standing because . . . [a] procedural violation was not itself an injury in fact."[101] The court held that plaintiff did not otherwise allege a risk of harm that satisfied the concreteness requirement. FACTA, a consumer protection statute, requires the truncation of consumer credit card numbers on printed receipts to "limit the number of opportunities for identity thieves to 'pick off' key card account information."[102] In this case, Kamal made several purchases at various J. Crew retail stores using a credit card. Upon each sale, Kamal received an "'electronically printed receipt' . . . that 'display[ed] the first six digits of [his] credit card number as well as the last four digits.'"[103] Kamal thereafter filed suit alleging J. Crew willfully violated FACTA by including the first six digits of his credit card number on his printed receipts.[104] The Third Circuit addressed the issue of whether a procedural violation alone presents a "material risk of harm" for the first time—in past cases decided by the circuit "the underlying harm contemplated by Congress had already

[98] *See In re Zappos*, 888 F.3d at 1026.
[99] Lawrence et al., *supra* note 82.
[100] *See id.*
[101] Kamal v. J. Crew Grp., Inc., 918 F.3d 102, 113 (3d Cir. 2019).
[102] *Id.* at 106–07.
[103] *Id.* at 107.
[104] *Id.*

materialized or failed to materialize."[105] Thus, the Third Circuit in *Kamal* was required to "consider the full reach of congressional power to elevate a procedural violation into an injury in fact."[106]

Applying the *Spokeo* Court's reasoning, the Third Circuit joined several of its sister circuits in requiring that an "'alleged procedural violation . . . manifest[s] concrete injury' if the violation actually harms or presents a material risk of harm to the underlying concrete interest."[107] If a procedural "violation does not present a 'material risk of harm to that underlying interest,'" then a plaintiff will fail to demonstrate a concrete injury.[108] Here, Kamal's alleged "concrete" injuries were "the printing of the prohibited information itself," and the "increased risk of identity theft" which resulted from the printing.[109] The Third Circuit held that neither of these alleged injuries satisfy the concreteness requirement of proving an injury in fact.[110] Although the Third Circuit acknowledged that Congress is "well positioned to identify intangible harms that meet the minimum Article III requirements," the court invoked *Spokeo*, stating that the violation of a procedural right granted by statute can be sufficient to constitute injury in fact, and a plaintiff "need not allege any *additional* harm."[111] However, the limitation here is that the phrase "additional harm" presumes that the plaintiff has suffered a *de facto* injury resulting from the procedural violation. The Third Circuit determined that the FACTA violation alleged by Kamal was not itself a concrete injury, and "does not present the circumstances envisioned by *Spokeo*."[112] Therefore, the court in *Kamal* concluded that J. Crew's violation of FACTA alone was insufficient to constitute an injury in fact.

Kamal also alleged that J. Crew's FACTA violation "created a real risk of identity theft," because receipts that are lost or discarded (e.g. thrown in the trash) could be used by identity thieves to obtain card information and commit identity theft.[113] The Third Circuit rejected this argument using similar reasoning to the Court in *Clapper* because the threat to Kamal's identity "consists of a highly speculative chain of future events."[114] The court determined that, absent a sufficient degree of risk, J. Crew's violation of FACTA was a "bare procedural violation" that did not create Article III standing.[115] This decision by the Third Circuit represents the alternative, less-consumer-friendly approach to standing in data-theft cases, requiring plaintiffs to allege some *additional* harm beyond the initial data breach itself in order to satisfy the injury-in-fact requirement.

[105] *Id.* at 112.
[106] *Id.*
[107] *Id.*
[108] *See id.* at 113.
[109] *Id.*
[110] *Id.*
[111] *See id.* at 113, 115.
[112] *Id.*
[113] *See id.* at 116.
[114] *See id.*
[115] *Id.* at 117.

D. EFFECTS OF THE CIRCUIT SPLIT

The use of disparate standards to satisfy the injury-in-fact requirement for standing in the different circuits has significant consequences for data breach litigation. Plaintiffs in the Sixth, Seventh, Ninth, and D.C. circuits face a lower threshold at the pleadings stage in order to get standing depending on the nature of the data breach—for some courts, the sole fact that a breach has occurred will be sufficient.[116] On the other hand, plaintiffs in the Second, Third, Fourth, and Eighth circuits face a higher bar to establish standing: simply alleging an injury based on the lone fact that a data breach has occurred will not satisfy the injury-in-fact requirement.[117] This disparity could result in significant inequities among similarly situated plaintiffs because factually similar cases could yield disparate outcomes based on the venue in which they are filed. Not only would this result in inequities among plaintiffs with factually similar cases, but such disparities might provide incentives for parties to engage in forum-shopping in order to obtain a desired outcome—a result that is inconsistent with basic principles of fairness.

E. A CIRCUIT SPLIT RIPE FOR RESOLUTION

The great data breach-standing circuit split, as illustrated above, is divided along the injury-in-fact requirement first defined in *Lujan* and then refined further by the Court in its subsequent decisions in *Clapper* and *Spokeo*.[118] Whereas the more consumer-friendly courts will treat an increased risk of future harm resulting from a data breach as an injury in fact, the opposing circuits have held that additional harm is required in order to pass muster. Given the latent nature of data-theft injuries, and the lack of comprehensive consumer protections in the current legislative scheme, the pro-consumer Sixth, Seventh, Ninth, and D.C. Circuit approach to standing in such cases appears to be the proper response to an emerging class of cases dealing with such injuries. A pro-consumer approach that treats an initial data breach as an injury sufficient to satisfy the injury-in-fact requirement for Article III standing would protect consumers in the absence of legislative action while also preserving the Supreme Court's injury-in-fact requirement defined in *Lujan*. The adoption of such an approach by the Supreme Court would resolve a circuit split, promote equitable resolutions to factually similar cases in different jurisdictions, and remove incentives for plaintiffs and defendants alike to engage in forum shopping and other inequitable behaviors.

---

[116] *See* Lawrence et al., *supra* note 82.

[117] *See id.*

[118] *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016); Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013); Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992).

VI. A JUDICIAL SOLUTION

A. THE ROLE OF THE SUPREME COURT

It may be incumbent on the judiciary to define the rights of data breach injury victims by establishing a procedural right to sue or enacting a comprehensive data privacy law in the absence of congressional action to define those rights. Given the ever-widening circuit split on the issue of standing in data breach cases, the Supreme Court has once again found itself in a position to offer guidance on the injury-in-fact requirement for Article III standing within the data breach context. In *Spokeo*, the Court issued a ruling that offered little clarity to lower courts attempting to apply its reasoning. The Court recognized that Congress had the power to "define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before," but also noted that "Congress'[s] role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right."[119] Thus, it is no wonder that courts have performed *Spokeo*'s concreteness analysis in an inconsistent manner, yielding unpredictable outcomes and a circuit split.

B. A POTENTIAL JUDICIAL SOLUTION TO THE CIRCUIT SPLIT

Should the Court revisit the question of standing, it should adopt a limited departure from the typical injury-in-fact requirement for Article III standing. In cases involving injuries alleged as a result of a data breach, the Court should establish clear guidelines for what will and will not be considered a legally cognizable injury. The Ninth Circuit's ruling in *Zappos* provides a model for what such a rule might look like—where there is a "credible threat of real and immediate harm"[120] stemming from a data breach, the injury-in-fact requirement will be satisfied in a data breach case. Adoption of a rule like this would not necessarily be out of line with the Court's past rulings. For example, the Court's decision in *FEC v. Atkins* is a case in which the violation of a procedural right granted under a statute was sufficient to satisfy the injury-in-fact requirement because it caused an injury of the type that Congress intended to prevent.[121] Where Congress has granted a procedural right to sue, a rule recognizing a data breach as an injury in fact should be given even greater deference because Congress's grant of such a procedural right is a clear signal that the legislature sought to vindicate the type of harm being addressed in the statute.

C. AN ALTERNATIVE, DEFERENTIAL JUDICIAL SOLUTION

In the alternative, if the Supreme Court chooses to address the circuit split by taking an approach that is more deferential to the legislature, the Court can look to Congress to circumscribe the limits of what constitutes an injury in fact. A deferential model would not be misaligned with the Court's

[119] *Spokeo,* 136 S. Ct. at 1550.
[120] *In re* Zappos.com, Inc., 888 F.3d 1020, 1027 (9th Cir. 2018).
[121] *See* FEC v. Akins, 524 U.S. 11, 20 (1998).

past rulings. For example, in the Court's *Lujan* concurrence, it noted that Congress "has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before."[122] Therefore, the Court and Congress would both be within the limits of their power if Congress were to pass a statute establishing a procedural right to sue in the event of a data breach, and the Court recognized the violation of such a statute as sufficient to satisfy the injury-in-fact requirement of Article III standing. The Court's adoption of a model of heightened deference to procedural rights granted by Congress would clearly define the rights of consumers and businesses alike, thus reducing transaction costs and confusion when a data breach occurs.

Providing additional support for the proposition that the Supreme Court is open to the idea of recognizing new rights of action is Justice Kennedy's *Lujan* concurrence, in which he stated, "As government programs and policies become more complex and far reaching, [the Court] must be sensitive to the articulation of new rights of action that do not have clear analogs in our common-law tradition."[123] Plaintiffs have attempted to analogize data breach injuries with common-law torts in order to gain standing, but courts have rejected arguments along these lines. For example, in *Kamal v. J. Crew Group, Inc.*, the court "rejected Kamal's argument that his alleged injuries were sufficiently concrete because they are analogous to common law privacy torts and actions for breach of confidence that are already recognized as providing grounds to sue, finding that his purported injuries didn't have the requisite 'close relationship' with these actions."[124] Thus, it seems unlikely that victims of data breaches will find redress by alleging a common-law tort claim. Instead, the Supreme Court can recognize that data breach injuries do *not* have an analog in common-law tort and defer to Congress where Congress has granted a statutory right to sue.

VII. A LEGISLATIVE SOLUTION

A. THE ROLE OF CONGRESS

Although Congress's role in identifying and elevating intangible harms does not mean that a plaintiff will automatically satisfy the injury-in-fact requirement whenever given a statutory right,[125] Congress is not powerless to provide a means by which the victim of a data breach can gain Article III standing when their injuries have yet to fully manifest. The Supreme Court has made it clear that "the . . . injury required by [Article] III may exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'"[126] Moreover, the Court has noted that "Congress may 'elevat[e]

[122] Lujan v. Defs. of Wildlife, 504 U.S. 555, 580 (1992) (J. Kennedy, concurring).

[123] *Id.*

[124] Allison Grande, *3rd Cir. Says J. Crew Receipt Row Doesn't Meet Spokeo Bar*, LAW360 (Mar. 8, 2019), https://plus.lexis.com/api/permalink/ff1c727b-3868-4585-a0bb-1aafe0a4eeb3/?context=1530671.

[125] *See Spokeo*, 136 S. Ct. at 1549.

[126] *Lujan*, 504 U.S. at 2145 (reiterating the principle that the injury-in-fact requirement may be satisfied by concrete, *de facto* injuries that previously were inadequate, but rise to the level of a legally cognizable injury upon Congress's creation of a legal right).

to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.'"[127] Thus, a strong precedential framework already exists for the Supreme Court to defer to Congress on whether an injury should be elevated to the status of a legally cognizable one.

B. A NARROWLY TAILORED LEGISLATIVE SOLUTION

A federal legislative solution could potentially take one of two forms: either Congress addresses data privacy issues on a case-by-case basis by passing a series of targeted laws, or Congress adopts a more comprehensive data privacy regime such as the GDPR recently enacted in the EU. With respect to the former, one potential solution is for Congress to establish procedural rights to sue when an information injury occurs, as in the case with FOIA, where "anyone whose request for specific information has been denied has standing to bring [suit]; the requester's circumstances . . . are irrelevant to his standing."[128] Congress could address certain, targeted, informational injuries in a manner similar to FOIA, where the violation of the statute itself recognizes an informational injury which, in the absence of the statute, would not have given rise to a legally cognizable injury. Doing so, however, would potentially run afoul of the requirement in *Spokeo* that a concrete injury is still required "even in the context of a statutory violation."[129] Therefore, Congress must make clear its intent to recognize data breach injuries as injuries in fact arising the moment the breach occurs, and thus bestow plaintiffs with the right to sue, not upon the theft of their SSN, the emptying of their bank account, or the ruination of their credit, but at the moment the plaintiffs become aware of a third party's mishandling of their personal information.

C. DETERRENCE: A COMPREHENSIVE LEGISLATIVE SOLUTION

As an alternative to a slew of narrowly targeted laws, Congress might be well advised to adopt a more comprehensive legislative solution, like the GDPR, to data privacy issues. Facilitating litigation by way of providing procedural rights, while a boon to the rights of data-theft victims, also carries with it large transactional costs and high barriers to entry for average Americans. Thus, a comprehensive solution to the issue of data breaches would also attempt to prevent them. Deterrence mechanisms could potentially be modeled after the GDPR, which allows for fines "up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher."[130] Providing for statutory penalties in the event of a data breach would serve multiple functions. First,

---

[127] *Spokeo*, 136 S. Ct. at 1549 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 578 (1992) to explain that Congress is well positioned to identify intangible harms that meet the minimum Article III requirements for standing and noting that Congress's judgment is "instructive and important").

[128] Zivotofsky *ex rel.* Ari Z. v. Sec'y of State, 444 F.3d 614, 617 (D.C. Cir. 2006) (providing an example of a statute where Congress has created a legal right, the invasion of which creates standing, even if the plaintiff would have not suffered a judicially cognizable injury without the statute).

[129] *Spokeo*, 136 S. Ct. at 577 (circumscribing the authority of Congress to identify and elevate intangible harms to satisfy the injury-in-fact requirement to attain Article III standing by stating that "bare procedural violations" are insufficient).

[130] Ben Wolford, *What Are the GDPR Fines?*, GDPR.EU, https://gdpr.eu/fines (last visited Mar. 4, 2021).

statutory penalties would function as a deterrent for the mishandling of data, and entities that collect, store, and process consumer data would be incentivized to employ more aggressive data-security protocols to avoid the imposition of a fine. Second, imposing fines on offenders serves as a warning to other companies to comply with the law or face fines; for example, commenting on GDPR fines levied against Marriott, Greenberg Traurig partner Paul Ferrillo stated, "The proposed fine against Marriott should serve as notice to other companies both under investigation now, and investigated down the road, that the fines and penalties provision of the GDPR is the real deal."[131] Finally, the imposition of fines introduces a public relations cost in addition to a monetary one; a company making headlines because it was fined for not complying with data privacy rules could deter customers from doing business with it in the future. Thus, a comprehensive data privacy solution would include statutory penalties in order to achieve maximum deterrence, as well as clearly define the rights of parties with respect to the handling of data, thereby making it easier for companies to conduct business and for consumers to know their rights.

VIII. CONCLUSION

Given the increasing importance of electronic data in modern life and the rapidity with which technological change is occurring, the time has come for an American data privacy solution. One avenue through which this can be accomplished is by the passage of a comprehensive federal data privacy bill such as the EU's GDPR. While single-state solutions have been slowly appearing, they risk creating a fragmented patchwork of data privacy protections that would prove confusing for consumers and corporations alike. Absent a legislative solution, however, a judicial solution may be a viable stop-gap option. A judicial solution to today's data privacy issues might include the Supreme Court's adoption of a model of standing that is more deferential to the judgment of Congress where it has established a procedural right to sue. Congress is well-positioned to identify new sources of data privacy injury as they arise, and, through a relaxed standing requirement, courts could be more receptive to the recognition of data breach injuries that have yet to fully manifest themselves because of the latent nature of these types of harms.

[131] Kate Fazzini, *Europe's Huge Privacy Fines Against Marriott and British Airways Are a Warning for Google and Facebook*, CNBC (July 10, 2019, 11:53 AM), https://www.cnbc.com/2019/07/10/gdpr-fines-vs-marriott-british-air-are-a-warning-for-google-facebook.html.