2018

Current Topics in Internet Law Data Breach Liability

Fadja Tassey

Introduction

A data breach is "the loss, theft, or other unauthorized access … to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data." [1] Though there are various ways in which personal information can be stolen, data breaches typically occur in one of three ways: (1) *hacking*, (2) *physical theft*, and (3) *point-of-sale attacks*.[2] Hacking, the most typical form of data breach, occurs when "hackers [access] a company's network and [steal] personal information." [3] Physical theft occurs when devices capable of data storage such as backup disks or laptops are

---

1 38 U.S.C. § 5727

2 Andrew Hoffman, 2 Years of Clapper: Takeaways From 12 Data Breach Cases, Law360 (Jan. 19, 2017, 5:52 PM), http://www.law360.com/ articles/621745/2-years-of-clapper-takeaways-from-12-data-breach-cases [https://perma.cc/SE4N-XY8Q].

3 Id.

stolen. [4] Point-of-sale attacks occur when data such as credit card information that is recorded and processed at the time of purchase is stolen.[5] In 2016 alone, millions of confidential records were compromised through these three types of data breaches. For instance, in March of 2016, Premier Healthcare reported a data breach, after a laptop computer which contained PHI of more than 200,000 patients was stolen from their billing department. In August of 2016, Oracle, the company that owns the MICROS point-of-sale system, used in more than 330,000 cash registers around the world, announced that its system had been hacked by a Russian cybercrime group. Then, in September of 2016, Yahoo announced that a hacker had stolen information such as e-mail addresses, passwords, full user names, dates of birth, and telephone numbers from at least 500 million accounts. When data is breached, businesses and financial institutions exhaust millions in financial resources to cover legal fees, fraud prevention, card reissuance, and lost revenue, while consumers, who also suffer loss of financial resources, are greatly disadvantaged by the fact that there are currently very few data breach liability remedies available.

The unavailability of legal remedies to properly address data breaches that occur with great frequency and regularity is commonly referred to as the *Data Breach Problem*. The recent frequency in data breaches over the past decade can be attributed to the fact that organized crime groups have now resorted to the theft and sale of personal information, finding it to be more reliable, safe, and lucrative than other types of organized crime. Moreover, in a technological age, the increased use of basic credit card transactions makes personal information more widely accessible to criminals--which, as a result, exposes businesses and consumers to a greater risk of

---

4 Id.

5 Id.

loss. The Privacy Rights Clearinghouse, a nonprofit privacy advocate site, reports that the 5,245 data breaches made public between 2005-2016, were comprised of over 900 million records. However, the number of records breached does not represent every single record breached during this period, since many organizations are not aware that their data has been breached or are not required to report the breach under state reporting laws. Despite the number and volume of data breaches that occur on an annual basis, the lack of consistent data protection creates significant economic concern for businesses and threatens consumer protection.

Part I of this note will expand on the data breach problem. Part II will discuss the current legal landscape of data protection in the United States. Part III will discuss the availability of civil remedies in data breach cases. Part IV will discuss recent attempts to pass comprehensive federal regulation. Part V will consider possible solutions to the data breach problem.

PART I.
The Data Breach Problem

Businesses use, store, and transfer sensitive information, both personal and financial, every day for legitimate business purposes and therefore are incentivized to protect such information in order to facilitate commerce. For instance, credit card information helps "process nearly $ 3.5 trillion per year. . . ." [6] However, one major factor prohibiting greater data protection, in hacking or point-of-sale attacks, is the inability to trace the point at which the data

---

[6] The Business of Banking: What Every Policy Maker Needs To Know, Am. Bankers Ass'n 1, 27 (Dec. 2016), http://www.aba.com/Tools/Economic/Documents/Businessofbanking. pdf.

was compromised. For instance, during an ordinary credit card transaction, a customer will provide their credit card information to the merchant company; the merchant company then reads and stores the card information; the information is transmitted to the merchant's acquiring bank, then the acquiring bank uses the information to verify the customer's account balance with the card-issuing bank; the card-issuing bank then releases the funds to the merchant. [7]If consumer data is compromised at any point during this long chain of transactions, it becomes nearly impossible to determine the source of the breach. Moreover, if, after acquiring it, the merchant company sells a consumer's data for profit, it will no longer be possible for the merchant company to monitor its management. As a result, the very mechanisms which help to facilitate commerce also lend to the widespread data protection issues. The complex legal questions and proof issues that arise from the lack of traceability in data breach cases is more cognizable under the common law. Victims of data breach are rarely, if ever, able to succeed under contract or tort causes of action since the contractual obligations are muddled when data is passed along multiple relationships. With data being transferred through multiple relationships, it is difficult for courts to determine who is obligated to whom. Therefore, the lack of traceability in data breach cases can create an almost insurmountable burden of proof for plaintiffs due to the fact that privity can potentially exist between multiple relationships: "card-issuing bank-customer, customer-merchant, merchant-acquirer bank, acquirer bank-card network, card network-card-issuing bank, or in the alternative, card-issuing bank-customer, customer-merchant, and merchant-integrated card network bank."[8] Another issue is that a lack of traceability creates a great incentive for

---

[7] R. Andrew Patty II, Credit Card Issuers' Claims Arising From Large-Scale Data Breaches, 23 J. Tax'n Reg. Fin. Instruments 5, 5, 8 (2015).

[8] R. Andrew Patty II, Credit Card Issuers' Claims Arising From Large-Scale Data Breaches, 23 J. Tax'n Reg. Fin. Instruments 5, 5, 8 (2015).

perpetrators to steal sensitive information without the consequence of criminal or civil liability. For instance, the sale of credit card numbers on the black market can net anywhere between $.50 and $48 per card.[9] Therefore, in the absence of adequate legal protections, the theft and sale of personal information serves as a very lucrative business for perpetrators---putting businesses and consumers at a greater risk of losing sensitive information.

PART II.
Laws Governing Data Security: State and Federal Laws

Despite the pervasiveness of the data breach problem, the United States currently does not have a comprehensive federal scheme to address the problem. However, privacy protection issues are addressed in a very limited sense through scattered federal regulations, constitutional rights, state notification laws, and the common law – all of which serve to partially address the data breach problem.

A. State Data Breach Protection

---

[9] Timothy Peacock & Allan Friedman, Automation and Disruption in Stolen Payment Card Markets, Workshop on Econ. Info. Security 1, 5-7 (May 11, 2014), http://weis2014.econinfosec.org/papers/PeacockFriedman-WEIS2014.pdf (noting that most loss occurs quickly after the breach occurs, so slow breach notification can significantly increase fraud success, increasing reimbursement costs).

The current state law framework provides consumer protection in the event of a data breach by way of notice to the consumer. Currently, 51 states and territories have enacted data-breach notification laws which require companies to notify its consumers within a certain timeframe that their personal information has been or may have been exposed. Most state notification statutes only provide consumer protection to the extent that notice helps to prevent against the future risk of fraudulent use of personal information. However, some state notification statutes provide a private cause of action which allow consumers to recover damages against the breaching company. The current state data breach notification scheme has proven problematic for businesses, since state notification laws vary from state to state. This lack of uniformity makes compliance burdensome and costly, particularly for national businesses that have nationwide consumer bases. One possible solution to this compliance issue is that the state data breach notification scheme should be preempted by comprehensive federal legislation, rather than continue to operate in a piecemeal fashion in conjunction with other federal data breach laws. Another possible solution is that a national business could simply comply with the strictest of all state notification laws in order to ensure compliance with the notification laws of all of the other states in which it has consumers. However, the dramatic differences among the state notification laws does not allow for this to be a feasible alternative. State data breach notification laws vary in some very significant respects: notification exemptions, timelines for notification, procedures for notification, penalties for failure to comply with the statute, and definition of personal information. The difference in the way in which *personal information* is defined by state notification statutes is split evenly among the states. Most states define *personal information* as: "(a) a first name . . . and last name in combination with any one or more of the following data elements, when the data element is not encrypted, redacted or secured by any other method

rendering the element unreadable or unusable: (i) social security number; (ii) a number on a driver license number. . . or number on a nonoperating identification license number; (iii) a financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual's financial account." [10]

However, 25 states define *personal information* more broadly to include passwords, PIN numbers, access codes for financial accounts, medical information, health insurance information, routing numbers in combination with the necessary access code or password, unique biometric data (such as fingerprints), and individual Taxpayer Identification Numbers.[11] Another significant difference among state notification statutes is whether or not they provide timeframes for notification. Most states do not provide specific timelines for notification, while seven states require businesses to notify consumers within 5 - 45 days after a breach has been discovered. Also, some states allow for delay beyond the statutory timeframe, if necessary for law enforcement to pursue an investigation. While most states don't provide a timeframe for notification, 41 states do, however, require analysis of the breach's risk of harm before determining whether notification is even necessary. [12] In these states, businesses are required to assess whether the breach "is likely to cause substantial economic loss to an individual" or whether "an illegal use of personal information has occurred, or is reasonably likely to occur"

---

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

[11] See, e.g., MD. CODE ANN., COM. LAW § 14-3501 (2013)

[12] *State Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGISLATURES (Jan. 19, 2017), http://www.ncsl.org/research/telecommunications-andinformation-technology/security-breach-notification-laws.aspx. A chart listing each of these states and their various statutory provisions regarding databreach notification may be found at DATA BREACH CHARTS,*supra* note 42.

before notice is required.[13] Therefore, businesses which have consumers in these states must comply with both of these requirements—notifying consumers within the statutory timeframe and not notifying consumers until a risk-of-harm analysis is completed. One commonality among state notification laws, however, is that they only require consumer notification "when the compromised data was not encrypted, or when the encryption key was also compromised." These provisions are referred to as the "encrypted data safe harbor."[14] Therefore, businesses with nationwide consumer bases are only required to contact consumers in instances where the breached data was not encrypted. Several states have attempted to address these compliance issues by allowing business that experience a breach which affects a certain number of people to simply post a notice on their website. [15] While substitute notice may be convenient for businesses, substitute notice is problematic for consumers who are unlikely to go on the company's website to see the notice. The current data breach notification scheme is also problematic for consumers because it reacts to data breaches rather than prevents them which, in effect, circumvents the legislative purpose of "allow[ing] consumers to protect themselves against identity theft" and "mitigat[ing] damages resulting" from data breaches.[16]

B. Federal Privacy and Data Security Laws

In addition to the state data breach notification scheme, consumers affected by a data breach are also entitled to relief under applicable federal laws. The current federal law framework is

---

13 HAW. REV. STAT. ANN. § 487N-1 (2009)

14 Jill Joerling, Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data, 32 WASH. U. J.L. & POL'Y 467, 475 (2010).

15 see, e.g., Customer Update on Data Breach, The Home Depot, https://corporate.homedepot.com/mediacenter/pages/statement1.aspx (last visited Sept. 8, 2015) (updating customers of a previous data breach through a posting on their website).

16 *Id.* at 471.

more industry-related than consumer related in that federal privacy and data security laws are narrowly tailored to prevent and protect breaches that occur in particular industries. For instance, the Computer Fraud and Abuse Prevention (CFAA) was passed by Congress in 1984 in an effort to criminalize hacking-- making it a crime to access, obtain information from, or use or transmit something to a computer in certain instances. The CFAA also provides victims of data breaches with a private cause of action in two limited circumstances: where a loss of at least $ 5,000 is aggregated over a one-year period or when there is damage affecting ten or more protected computers within a one-year period.[17] Theoretically, the CFAA has great potential to provide a remedy to consumers in a typical data breach case because it's scope broadly encompasses any computer "which is used in or affect[s] interstate or foreign commerce or communication",--- which is any computer with internet access. [18] However, the CFAA has rarely been successful in protecting victims of data breaches because of its requirement of a showing of substantial economic harm. In two cases where the CFAA's private right of action was brought in regard to an asserted data breach, the claims were dismissed because the plaintiffs could not show that they had suffered $ 5,000 in damages.[19] Moreover, the CFAA limits its application by prohibiting private actions against entities for "negligent design or manufacture of computer hardware, computer software, or firmware."[20] Congress also passed the Electronic Communications Privacy Act of 1986 (ECPA)[21] in an effort to protect individuals from

---

17 18 U.S.C. §1030(c)(4)(A)(i)

18 18 U.S.C. §1030(e)(2)

19 See In re Google Android Consumer Priv. Litig., 2013 WL 1283236; In re iPhone Application Litig., 844 F. Supp. 2d 1040 (N.D. Cal. 2012)

20 18 U.S.C.A. §1030(g)

21 Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.)

government eavesdropping and other intrusions. As a communications privacy protection law, the ECPA makes it illegal to intercept wire, oral, or electronic communications, except if such actions are taken by a law enforcement agency with judicial approval. The ECPA also regulates the privacy of and government access to stored electronic communications. The Health Insurance Portability and Accountability Act of 1996 (HIPPA)[22], one of the most significant federal health care privacy and data security laws governing the healthcare industry to date, protects individuals against the unauthorized access of "individually identifiable *health* information" relating to: [an] individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.[23] HIPPA's *Standards for Privacy of Individually Identifiable Health Information* ("Standards") established national standards to protect individuals' personal health information by requiring health plans, health care clearinghouses, and health care providers that conduct certain health care transactions electronically to follow appropriate safeguards to protect the privacy of such information, and by placing limits and conditions on the uses and disclosures of such information without patient authorization.[24] HIPAA does not, however, provide individuals with a private cause of action for violations of its Standards. Rather, HIPAA, allows for the Office for Civil Rights to impose a civil monetary

---

22 Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C.)

23 Summary of the HIPPA Privacy Rule, U.S. DEPT OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

24 Id.

penalty of $ 50,000 for each violation of it Standards. HIPAA also allows for criminal prosecution against entities that commit specific types of violations of its Standards. Congress has also passed a number of financial data laws, such as the Gramm-Leach-Bliley Act of 1999 (GLBA)[25] and the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"). [26] GLBA regulates how financial institutions handle, store, and disclose individuals' personal financial information. GLBA consists of three parts: (1) the Financial Privacy Rule, which sets out how the information is to be collected and disclosed by a financial institution; (2) the Safeguards Rule, which mandates that financial institutions adopt security measures to protect the information; and (3) the Pretexting Provisions, which prohibit the use of false pretenses in order to access the information.[27] Financial institutions that violate GLBA can face civil penalties of anywhere up to $100,000 per violation while officers and directors of such institutions are also subject to face civil penalties of up to $10,000 per violation. GLBA also provides criminal penalties against anyone who knowingly and intentionally obtains customer information through the use of false pretenses. Finally, Congress passed the FACT Act with the legislative purpose of preventing identity theft and providing consumers with better access to their credit reports.[28] The

---

[25] Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.)

[26] The Fair Credit Reporting Act was originally passed in 1970 to regulate consumer reporting agencies' use of sensitive consumer information. 15 U.S.C. §§ 1581--1597. The Act had three main goals which included: (1) increasing transparency in the industry for consumers; (2) protecting consumers from the damages of incorrect information; and, (3) improving the accuracy of credit reports. Meredith Schramm-Strosser, The "Not So" Fair Credit Reporting Act: Federal Preemption, Injunctive Relief, and The Need To Return Remedies For Common Law Defamation To The States, 14 DUQ. BUS. L.J. 165, 170 (2012).

[27] Margaret Rouse, Gramm-Leach-Bliley Act (GLBA), TECHTARGET, http://searchcio.techtarget.com/definition/Gramm-Leach-Bliley-Act (last visited Jan. 19, 2017)

[28] (THE CATHOLIC UNIV. OF AMERICA, OFFICE OF GENERAL COUNSEL: SUMMARY OF FEDERAL LAWS, http://counsel.cua.edu/fedlaw/fcra.cfm)

Red Flags Rules of 2007 help carry out the FACT Act's legislative purpose of preventing identity theft by requiring certain institutions to "identify and respond to account activities that are possible indicators 'red flags' of identity theft . . . ." [29]

PART III.
Civil Remedies

In addition to the limited protections provided under state and federal laws, civil remedies provide little relief to victims of data breach cases. Generally, injured parties are entitled to civil remedies, in either state or federal court, through various legal remedies such as: breach of contract, breach of implied contract, breach of fiduciary duty, negligence, public disclosure of private facts, and emotional distress. However, these claims only tend to be successful in cases where the breaching company has not provided timely notification.[30] Moreover, tort remedies are rarely, if ever, successful in data breach cases, since the economic loss doctrine bars recovery where only purely economic losses are asserted. For instance, *In re Michaels Stores PIN Pad Litigation*, held that claims of negligence and negligence per se could not survive dismissal when personal injury or property damages could not be demonstrated and only increased risk of identity theft and economic loss damages were alleged."[31] Similarly, in *Rowe v. UniCare Life and Health Insurance Co.,* held that in a tort action, damages for emotional distress could only be recovered if the plaintiff could show "he suffered from some present injury beyond mere

---

[29] Yoon-Young Lee, FACT Act "Red Flag" Rules, WILMERHALE (Sept. 2, 2008), http://www.wilmerhale.com/pages/publicationsandNewsDetail.aspx?NewsPubId= 91356.

[30] Timothy H. Madden, Data Breach Class Action Litigation--A Tough Road for Plaintiffs, 55 FALL Bos. B.J. 27, 29 (2011); see also In re Michaels Stores Pin Pad Litig., 830 F. Supp. 2d at 527--28, 531 (allowing claims under breach of implied contract and the Illinois Consumer Fraud and Deceptive Business Practices Act to stand, citing the fact that Michaels did not timely notify its customers of the data breach in its reasoning for upholding both claims).

[31] In re Michaels Stores Pin Pad Litig., 830 F. Supp. 2d at 526, 531.

exposure of his information to the public."[32] Claims for breach of fiduciary duty also tend to be unsuccessful due to the lack of fiduciary obligation between the consumer and the breaching company.[33] For instance, in *Andersen v. Hannaford Brothers Co*., plaintiff's debit card information was compromised after defendant's electronic payment process system was hacked, however the First Circuit dismissed plaintiff's claim for breach of fiduciary duty, holding that in order to establish a fiduciary duty a plaintiff must: "(1) allege 'the actual placing of trust and confidence' in the defendant; (2) 'show that there is some disparity in the bargaining positions of the parties;' and (3) show 'that the dominant party has abused its position of trust.'" [34] The First Circuit found that, because *Andersen* involved a grocery store, there was nothing but a fair exchange of groceries for money, and there was no evidence that the defendant had taken advantage of the plaintiff. On the other hand, breach-of-implied-contract claims have shown some success in the data breach context. In *Anderson,* the First Circuit, found that an implied contract to safeguard data could exist between consumers and companies they purchase from since the company would "not use the credit card data for other people's purchases, would not sell the data to others, and would take reasonable measures to protect the information." [35]The breach-of-implied-contract remedy therefore appears to be limited when a company has taken reasonable measures to protect the consumer information. Another issue that plaintiffs of data breach cases face, in addition to a limited likelihood of success on the merits, is an inability to meet the standing requirement in federal courts. The standing requirement comes from Article III

---

[32] Rowe v. UniCare Life & Health Ins. Co., No. 09-C-2286, 2010 WL 86391, at *6 (N.D. Ill. Jan. 5, 2010).

[33] IAN C. BALLON, E-COMMERCE & INTERNET LAW 27.07 (2d ed. 2013)

[34] Andersen v. Hannaford Bros. Co., 659 F.3d 151, 157 (1st Cir. 2011).

[35] Id. at 159.

of the U.S. Constitution.[36] In order to bring a "case or controversy" in federal court, a plaintiff must satisfy three elements of standing: First, the plaintiff must have "suffered an 'injury in fact'--an invasion of a legally protected interest." The injury complained of must be "actual or imminent, not "conjectural' or "hypothetical."' Second, a plaintiff's claim must arise from an injury that "fairly can be traced to the challenged action of a defendant." Third, a favorable court decision must be able to redress the plaintiff's injury. The plaintiff bears the burden to establish all three elements.[37] Generally, the first element—the "injury in fact" requirement—is the most difficult to establish in data breach cases since it requires plaintiffs to show they suffered an "actual or imminent" injury. In data breach cases, establishing an *actual* injury tends to be problematic because many credit companies and financial institutions will refund and void fraudulent purchases as a matter of industry practice. So, while one might feel troubled after learning their personal information has been compromised, the legitimacy of this concern is minimized by the inability to establish an *actual* injury in federal court. Plaintiffs who seek relief in federal court are therefore left with the alternative option of claiming that they will suffer an *imminent* injury from the breach. Indeed, a consumer whose personal information is compromised is now at a greater risk of becoming a victim of identity theft at some point in the future. However, the Supreme Court's interpretation of standing in *Clapper v. Amnesty International* has made it difficult for plaintiffs with claims of an *imminent* future injury to the satisfy standing requirement.[38] In Clapper, plaintiffs were lawyers, human rights researchers, and

---

[36] U.S. Const. art. III §2.

[37] Patricia Cave, Comment, Giving Consumers a Leg to Stand On: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits, 62 Cath. U. L. Rev. 765, 772 (2013) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992)).

[38] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1149-50 (2013).

journalists who worked with certain foreign clientele that could have been subject to U.S. government surveillance under the Foreign Intelligence Surveillance Act of 1978 ("FISA").[39] Plaintiffs attempted to bring a claim to challenge Section 702 of FISA (" § 1881a") -- which allows the government to obtain foreign intelligence information on foreign powers and those associated with foreign powers for national security purposes.[40] Plaintiffs needed to communicate regularly with people subject to government surveillance under § 1881a for work related purposes but were forced to stop certain telephone and e-mail conversations and use alternative methods of communication, such as traveling abroad to have in person conversations, in order to avoid being targeted under § 1881a.[41] The plaintiffs asserted two separate theories of Article III standing: (1) they would suffer injury because there was "an objectively reasonable likelihood that their communications [would] be acquired under § 1881a at some point in the future," and (2) they had already suffered injury because "the risk of surveillance under § 1881a [was] so substantial that they had been forced to take costly and burdensome measures to protect the confidentiality of their international communications."[42] The Court ultimately ruled that the plaintiffs failed to satisfy the "injury in fact" requirement for standing. The Court reasoned that plaintiffs failed to establish that the government surveillance caused an *actual* injury or an *imminent* future injury since any potential future injury depended on the occurrence of a "highly attenuated chain of possibilities."[43] As the Court explained, plaintiff's argument required a long

---

[39] Id. at 1157.

[40] Id. at 1142.

[41] Id. at 1157.

[42] Id. at 1146.

[43] Id. at 1148

chain of inferences: (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts. [44] Some courts have viewed Clapper as imposing a very rigorous standard for plaintiffs alleging future injury of identity theft, while others distinguish Clapper as unique on its facts. The latter interpretation makes most logical sense since the plaintiffs in Clapper merely suspected that the government intercepted their communications with potential terrorists; however, in data breach cases the threat of future harm is not nearly as speculative since the data has already been stolen or compromised. *Lewert v. P.F. Chang's China Bistro, Inc.*, illustrates the chilling effect that Clapper had on granting standing in data breach cases.[45] In Lewert, the plaintiffs alleged injury stemming from a data breach at P.F. Chang's that compromised an estimated seven million cards.[46] The Seventh Circuit, however, dismissed plaintiff's claims about increased risk of identity theft in the future, reasoning that the harm was not "imminent" since it could take several years to occur, and that "there is no reason to believe that identity theft protection was necessary" after the cancellation

---

[44] Id.

[45] Lewert v. P.F. Chang's China Bistro, Inc., No. 14-CV-4787, 2014 WL 7005097, at 1, 4 (N.D. Ill. Dec. 10, 2014).

[46] Id.

of a debit card.[47] After Clapper, *Remijas v. Neiman Marcus Group, LLC* was the first appellate court case to provide a breakthrough toward establishing standing in data breach cases. In Remijas, Neiman Marcus customers brought a class action suit against Neiman Marcus after a company cyberattack caused fraudulent charges to appear on their credit cards.[48] The plaintiffs asserted two imminent injuries: "an increased risk of future fraudulent charges and greater susceptibility to identity theft."[49] Though the district court dismissed plaintiffs' complaint based on a narrow reading of Clapper as foreclosing the use of future injuries to establish Article III standing in data breach situations, the Court of Appeals for the Seventh Circuit read Clapper more broadly. The court distinguished Remijas from Clapper based on the differences in facts. The court stated that the threat of potential injury to plaintiffs was reasonably likely to occur because making fraudulent charges or assuming the plaintiffs' identities was the very reason why hackers stole credit card information from Neiman Marcus in the first place. [50]The court also held that the two other requirements of standing, causation and redressability, were satisfied.[51] As for the causation element, the court was liberal in finding that Neiman Marcus's malware possibly caused plaintiff's information to be exposed--though one could argue that hackers obtained the credit card information through other avenues.[52] In regards to redressability, the court reasoned that plaintiffs would benefit from a favorable decision since there was no

---

47 Id.; Note that the Seventh Circuit reversed and remanded Lewert v. P.F. Chang's China Bistro, Inc. recently in April 2016 following the Remijas standard. Lewert v. P.F. Chang's China Bistro, Inc., No. 14-3700, 2016 WL 1459226 (7th Cir. Apr. 14, 2016).

48 Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

49 Id. at 692.

50 Id. at 693.

51 Id. at 696-97.

52 Id.

guarantee that the injuries plaintiffs suffered or would suffer would be fully reimbursed, due to a variety of restrictions on credit card and debit card liability rules regarding prompt reporting and other variables. [53] In sum, the Seventh Circuit's approach to standing in Remijas provides plaintiffs in data breach cases with a greater chance of bringing a claim in federal court. Although civil remedies might not be the ultimate solution to the data breach problem, the adoption of a more relaxed standing requirement is an effective method to address the data breach problem within the current legal framework. In addition, a more relaxed standing requirement allows for more class actions to be brought against big businesses. Class actions have traditionally served as a powerful tool for consumers to keep big corporations responsible. Any increased ability to utilize class actions also serves as a potentially useful vehicle for moving towards regulatory reform, since successful data breach class action suits, and subsequent pushback by companies who have to bear the financial burden without adequate guidelines, will hopefully generate enough momentum for the federal government to move towards a more comprehensive regulatory solution. [54]

PART IV.

---

53 Id.

54 2016 COLUM. BUS. L. REV. 544

Attempts to Pass Comprehensive Federal Legislation

Despite the existence of various federal laws which aim to protect consumer data and privacy in specific industries or instances, Congress has not yet been successful in creating a uniform standard to addresses consumer data protection in all industries, partly because of the difficulty of gaining bipartisan support. While Democrats and Republicans could agree that there is a need for a more uniform standard, constant division on the substantive aspects of proposed data protection laws has prevented Congress from setting a uniform standard. The current patchwork of state laws and industry-related federal laws governing data protection in the U.S. is therefore due to the numerous policy disagreements on the data breach problem. Hence, recent attempts to pass uniform data protection laws have resulted in a substantive compromise of a proposed bill. For instance, several of the cybersecurity and data privacy bills that were introduced in the 113th Congress needed to be compromised in scope for them to even have a chance of gaining bipartisan support. The Cybersecurity Enhancement Act of 2014 was one of the few data security bills introduced in the 113th Congress which successfully passed into law.[55] The Cybersecurity Enhancement Act was originally proposed as a bill which aimed to address cybersecurity issues by giving regulatory power to the National Institute of Standards and Technology to develop "voluntary, industry-led set of standards…to cost effectively reduce cyber risks to critical infrastructure." [56] The Cybersecurity Enhancement Act easily received bipartisan support, partially because it delegates regulatory authority to a private entity rather than to federal or state agencies, but also because it left out certain sections which potentially could have provided even

---

[55] Cybersecurity Enhancement Act of 2014, S. 1353, 113th Cong. (2014), https://www.congress.gov/bill/113th-congress/senate-bill/1353.

[56] Cybersecurity Enhancement Act of 2014, S. 1353, 113th Cong. § 101(a)(2) (2014)

greater data security---such as, a comprehensive data-sharing plan that would facilitate cooperation between companies and the government to combat breaches. [57] This very same comprehensive data-sharing plan was later included in the Cybersecurity Information Sharing Act of 2014, which partly explains why this Act didn't gain the support it needed to become law. The Cybersecurity Information Act of 2014 aimed to provide cybersecurity and encourage the sharing of consumer data between businesses, including government and private businesses, by authorizing private entities to monitor information systems and share any potential cybersecurity threat indicators. [58] Despite its well-intended purpose, privacy protection advocates strongly opposed the bill out of fear that allowing "cybersecurity information" to be shared between government and businesses and authorizing private entities to monitor personal information, would also authorize the government to request that private entities provide it with access to a wide variety of personal information, which could be used in criminal proceedings. [59] Privacy advocates feared that bill would effectively allow the government to circumvent the privacy protections provided for in the Electronic Communications Privacy Act. Another reason that contributed to the bill's lack of support is that it provided civil immunity to the private entities that were supposed to monitor sensitive information or share threat indicators. Proponents of the bill argued that immunizing businesses from liability would further the bill's purpose of encouraging information sharing between businesses. However, opponents believed that providing civil immunity to businesses would undercut the bill's intended purpose of providing

---

57 See e.g; §III (B)(2) of the Cybersecurity Information Sharing Act of 2014.

58 Cybersecurity Information Sharing Act of 2014, S. 2588, 113th Cong. (2014), https://www.congress.gov/bill/113th-congress/senatebill/2588/actions.

59 Sandra Fulton, Beware the Dangers of Congress' Latest Cybersecurity Bill, Am. Civil Liberties Union, https://www.aclu.org/blog/beware-dangers-congress-latest-cybersecurity-bill.

greater cybersecurity since immunization could potentially eliminate the accountability businesses owe consumers and would also encourage businesses to share data without consumer authorization. The Personal Data Privacy and Security Act of 2014 was another bill introduced in the 113th Congress that failed to become law due to a lack of bipartisan support.[60] The Personal Data Privacy and Security Act of 2014 aimed to provide greater consumer privacy protection by providing increased punishments for data privacy violations, such as identify theft and willful concealment of breaches, requiring business participation in a security program, and instituting a sixty-day timeline within which businesses and federal agencies must disclose breaches to individuals whose personally identifiable information had been compromised. [61] Unsurprisingly, this bill did not pass into law due to strong congressional disagreements. The Data Security Act of 2014 aimed to provide consumer protection by requiring businesses to notify consumers of security breaches.[62] One criticism that prevented this bill from becoming law was that it did not mandate businesses to follow any mandatory security procedures, but instead gave businesses too much discretion to create and follow their own "reasonable" security policies and procedures. Another criticism to the bill was that it contradicted its own legislative purpose of providing consumer protection since it did not allow consumers to bring a private right of action for violations of the Act in state court, denying consumers of legal remedies it intends to provide. The Data Security and Breach Notification Act of 2014 attempted to create a uniform standard for data breach notification.[63] The Act would have given the Federal Trade Commission (FTC)

---

60 Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014)

61 Id.

62 Data Security Act of 2014, S. 1927, 113th Cong. (2014).

63 Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (2014).

power to set security standards for businesses that possessed personal information along with the power to set a strict thirty-day notification standard. [64] The Act also gave the United States Secret Service and the Federal Bureau of Investigation enforcement power to criminalize any "intentional or willful" concealment of a breach that results in economic harm of at least $1000. [65] This provision had potential to be very effective in encouraging businesses to notify affected consumers immediately after a breach is discovered. Another potential benefit under the Act is that it would have preempted the scattered state notification scheme and provided national businesses with a more clear and uniform standard. Unfortunately, the bill was unable to gain the Republican support it needed since it conflicted with a similar Republican proposed bill. The conflicting bill sought to give the Federal Trade Commission enforcement power against businesses who failed to take reasonable steps to protect personal data—without giving the FTC any additional power to set standards for data security. [66]The Personal Data Protection and Breach Accountability Act of 2014 aimed to protect consumer data through setting a series of safeguards for business entities to follow in their data privacy programs and strict penalties for businesses that did not properly protect personal information or timely notify customers of a breach of their information. [67] The provisions in this bill were extremely consumer friendly: authorized punishment for intentional or willful concealment of a data breach of personal information; private causes of action for the willful concealment of a data breach with no dollar

---

64 Id.

65 Id.

66 Alexei Alexis, Data Security Outlook Remains Uncertain Despite Flurry of Bills, Bloomberg BNA (Apr. 22, 2014), http://www.bna.com/datasecurity-outlook-n17179889758; see Data Security and Breach Notification Act of 2013, S. 1193, 113th Cong. (2013)

67 Personal Data Protection and Breach Accountability Act of 2014, S. 1995, 113th Cong. (2014)

amount requirement; private causes of action for economic harm or "substantial emotional distress" to at least one person; remedies following a breach such as free credit monitoring services, a security freeze on the individual's credit report, and a reimbursement of costs resulting from the breach, including costs resulting from identity theft; individuals would be allowed to bring suits for damages of up to $ 20,000,000 as well as punitive damages for willful or intentional violations.[68] Unfortunately, the bill did not pass, and it died with the adjournment of the 113th Congress. Still, one can predict that the bill would have received strong opposition from business focused organizations since they would have to bear most of the burden of this consumer-friendly legislation. Recent measures proposed during the 114th Congress have aimed to address the issues that prevented the passage of earlier bills. For instance, President Obama recently proposed the Personal Data Notification & Protection Act of 2015 during the 114th Congress as another attempt to pass a uniform breach notification law. [69] The Personal Data Notification & Protection Act contains similar parts of other bills, but applies to a wider range of personal information including: (1) first and last name in combination with several different elements, (2) a government-issued identification number, including a social security number or driver's license number, (3) biometric data including fingerprints or voice prints, (4) unique account identifiers, and (5) a username in combination with a password or security question.[70] The bill also gives the Federal Trade Commission rulemaking authority and sets a strict standard of notification to the Federal Trade Commission--thirty days after the entity discovers the breach. The Personal Data Notification & Protection Act has an exception that does not require

---

[68] Id.

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

[70] Id.

companies to disclose breaches unless there is a reasonable risk that the individuals whose data was affected will be harmed (similar to the risk analysis provisions found in some state notification laws). Also, the Federal Trade Commission and state Attorneys General would handle the enforcement of the provisions of this Act. The Personal Data Notification & Protection Act contains a range of much needed data security provisions, but as is often the case it only takes one small provision to derail the whole thing. However, even if not adopted in its entirety, the Act sets a high standard for the definition of sensitive personally identifiable information and notification deadlines. The Data Security and Breach Notification Act of 2015 is another bill that was introduced during the 114th Congress. [71] This Act gives the Federal Trade Commission rulemaking authority over information security; and requires notification in at least 30 days, unless notice would not be feasible. [72] The Act also preempts state laws relating to data security and breach notification, but it does not preempt state law tort, contract, trespass, or fraud claims. Considering the concerns surrounding the failed bills of the 113th Congress, the Data Security & Breach Notification Act of 2015 could serve as a compromise for passing the comprehensive data security and breach notification law that the United States needs.

---

71 Data Security and Breach Notification Act of 2015, S. 177, 115th Cong. (2014).

72 Id.

PART V.
Potential Solution to the Data Breach Problem

The data breach problem is of paramount concern to businesses and consumers who, in a global economy, use, store, and access sensitive information every day. The increased frequency and regularity of data breaches proves that the current patchwork of state and federal laws does not effectively address or prevent the widespread data security issues in the U.S. Hence, a clear uniform legal standard for breach notification and comprehensive data security is much needed. Although Democrats and Republicans tend to be divided in the area of data security and breach notification, it is possible to achieve bipartisan support by adopting rules from some of the failed data security and breach notification bills. Given the vast differences in state notification laws across the country, Congress should prioritize adopting a comprehensive breach notification law. Congress should develop a strong breach notification standard like that in the Personal Data Notification and Protection Act, so that the federal standard would be closer to even the strictest of state standards. The Data Security & Breach Notification Act of 2015 is a good attempt to reach a compromise on the issues that divide Democrats and Republican with regard to breach notification. Moreover, if this Act were to be enacted it would preempt scattered state laws, and therefore provide more uniformity. However, breach notification only matters when the breach has already occurred, and it does little to prevent breaches. A comprehensive data security legislation that gives regulatory and rulemaking authority to the Federal Trade Commission to create broad security standards but which allows business to develop their own data security procedures. Greater federal regulation is needed for businesses to improve their methods of

handling sensitive, personal information. In addition, federal regulation should require there to be more transparency regarding the data security practices that each business practices so that consumers can know exactly what data security practices each company uses to protect their personal information, and how those procedures compare to national or industry norms. There also needs to be a clear private right of action under a federal data privacy law. For example, a negligence cause of action which would create a duty for the company to protect a customer's data when it is given to them. When the company does not take sufficient measures to protect the data, it has breached its duty to the consumer. A data security law that provides a cause of action for negligence could avoid additional federal regulations since companies would then have every incentive to handle personal information as securely as possible, without clear regulation.