SO YOU'VE BEEN NOTIFIED, NOW WHAT? THE PROBLEM WITH CURRENT DATA-BREACH NOTIFICATION LAWS

Rachael M. Peters*

Data breaches, now a common occurrence throughout the world, are an ever-present threat to both consumers and companies, exposing on average the personal information of 1.1 million people and racking up costs of about $5.4 million with each occurrence. This problem is further exacerbated by the current data-breach notification regime, which consists of 47 various, sometimes conflicting, state laws. Thus, when a data breach does occur, companies must consult the state law of each affected consumer to determine whether that consumer must be notified, and when notification must occur. This may be extremely burdensome for large, nationwide companies with thousands or even millions of consumers in multiple states. Most importantly, even when these various state data-breach laws are effective and consumers are notified of a breach, they have almost no legal recourse against the entity whose security breach led to the unlawful or unauthorized procurement of their personal information. There is no clear-cut state or federal civil cause of action for consumers to bring, and existing causes of action have had limited success when applied to data breaches due to issues with standing and injury. Therefore, a stronger data-breach notification regime that provides consumers with a remedy when a data breach does occur and that is more effective in preventing data breaches from happening should be considered. In this way, consumers will be better protected and the damage caused by data breaches in the future will be minimized.

TABLE OF CONTENTS

---

* J.D. Candidate, University of Arizona James E. Rogers College of Law, 2015. I would like to thank Derek Bambauer for graciously sharing his knowledge, guidance, and advice in the writing and development of this Note. A special thank you is also extended to Justin DePaul and David Udall for their time and assistance in editing, as well as for the invaluable feedback they provided. Finally, I would like to thank my parents, George and Debbie Barnes, for always supporting me in all of my endeavors and for their unconditional love and encouragement.

INTRODUCTION

Recently, data breaches have become an enormous and costly problem for both corporations and consumers. Hardly a day passes without a data breach, and many remain undiscovered for months or even years.[1] Between January 2005 and June 2013, there were approximately 3,763 known data breaches with an estimated 608 million records containing sensitive "personal information"[2] compromised in

1. Robert Hamilton, *Mistakes are Costing Companies Millions from Avoidable Data Breaches*, SYMANTEC (June 5, 2013), http://www.symantec.com/connect/blogs/mistakes-are-costing-companies-millions-avoidable-data-breaches; VERIZON, 2013 DATA BREACH INVESTIGATIONS REPORT 8 (2013). The latest daily data breaches may be found on SC Magazine's Data Breach Blog. *The Data Breach Blog*, SC MAGAZINE, http://www.scmagazine.com/the-data-breach-blog/section/1263/# (last visited Oct. 27, 2014).

2. "Personal information" is defined by each individual state's data-breach notification statute. Though states' definitions vary, they commonly include the consumer's first and last name in combination with either their social security number, driver's license or state identification number, or any financial information—which may include a debit card, credit card, or bank account number. It is this information, when breached, that will trigger data-breach notification laws. Reid J. Schar & Kathleen W. Gibbons, *Complicated Compliance: State Data Breach Notification Laws*, BLOOMBERG LAW (Nov. 11, 2013, 9:41 AM), http://about.bloomberglaw.com/practitioner-contributions/complicated-compliance-state-data-breach-notification-laws/. *See infra* Part I.B for additional information on state definitions of "personal information."

the United States alone.[3] Furthermore, it is estimated that, in the average data breach, 1.1 million identities are exposed at a cost of approximately $157 per record, for a total cost of around $5.4 million per breach.[4]

These data breaches occur as a result of either human or system error, or criminal activity.[5] One prominent headline in early 2014 was Target's massive data breach involving the personal information of approximately 70–110 million customers during the 2013 holiday season.[6] This breach occurred through the use of malware, which infected Target's credit-card-processing system and was able to obtain information from the magnetic strips on customers' debit and credit cards.[7] Stolen information included customers' names, addresses, phone numbers, email addresses, credit and debit card numbers, and encrypted PIN numbers.[8]

Suffering a similar security breach, Home Depot revealed in September 2014 that as many as 56 million customers' account information had been compromised when those customers had used their debit or credit cards to make purchases in the company's various stores.[9] Like Target's, this breach occurred through the use of malware installed on the company's cash register system.[10]

Another sizeable data breach, disclosed in October 2014, affected the customers of JP Morgan Chase who had utilized the company's online services.[11] There, the contact information of 76 million households and 7 million small businesses was compromised.[12] And, although the exposed information included only names, addresses, phone numbers, and email addresses—not account numbers, birth dates, social security numbers, passwords, or user IDs—JP Morgan Chase still advised its customers that the accessed information could be used to

---

3. *Data Breach Trends & Stats*, IN DEFENSE OF DATA (Oct. 12, 2013, 7:34 AM), http://www.indefenseofdata.com/data-breach-trends-stats/ (citing PRIVACY RIGHTS CLEARING HOUSE, A CHRONOLOGY OF DATA BREACHES (2013)).

4. *Id.* (citing SYMANTEC, INTERNET SECURITY THREAT REPORT VOLUME 17 (2012); PONEMON INST. & SYMANTEC, 2013 COST OF A DATA BREACH: GLOBAL ANALYSIS (2013)); Hamilton, *supra* note 1.

5. *Data Breach Trends & Stats*, *supra* note 3 (citing PONEMON INST. & SYMANTEC, 2013 COST OF A DATA BREACH: GLOBAL ANALYSIS (2013)).

6. Javier E. David & Izzy Best, *Target: Stolen Information Involved at Least 70 Million People*, CNBC (Jan. 10, 2014, 1:34 PM), http://www.cnbc.com/id/101323479.

7. Rachel King, *Target's Data Breach: Yes, It Gets Worse*, CNET (Jan. 18, 2014, 12:09 PM), http://news.cnet.com/8301-1009_3-57617447-83/targets-data-breach-yes-it-gets-worse/. Additional information about the malware used in the attack can be found in Brian Krebs, *A First Look at the Target Intrusion Malware*, KREBSON SECURITY (Jan. 15, 2014), http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/.

8. Paula Rosenblum, *The Target Data Breach is Becoming a Nightmare*, FORBES (Jan. 17, 2014, 2:22 PM), http://www.forbes.com/sites/paularosenblum/2014/01/17/the-target-data-breach-is-becoming-a-nightmare/.

9. Toby Talbot, *Home Depot Confirms Largest Retail Data Breach*, N.Y. TIMES, Sept. 19, 2014, at B3.

10. *Id.*

11. Larry Magid, *JP Morgan Chase Warns Customers About Massive Data Breach*, FORBES (Oct. 2, 2014, 5:56 PM), http://www.forbes.com/sites/larrymagid/2014/10/02/jp-morgan-chase-warns-customers-about-massive-data-breach/.

12. *Id.*

facilitate phishing scams, in which customers could be prompted to provide additional sensitive personal information.[13]

Criminal attacks, like those experienced by Target, Home Depot, and JP Morgan Chase, tend to be opportunistic, targeting easily exploited data rather than specific individuals.[14] It is estimated that this type of cybercrime will continue to grow at an annual rate of 10% each year through 2016.[15]

However, two-thirds of data breaches are actually caused by human or system error.[16] These incidents commonly occur in situations where: (1) employees do not properly handle information; (2) government and industry regulations are violated; (3) hardware, such as a laptop with unencrypted information, is stolen due to employee or employer negligence[17]; (4) unauthorized access to data is permitted; or (5) a data dump inadvertently occurs.[18] With these types of statistics, it is no wonder that privacy concerns regarding the Internet have risen from 33%–50% since 2009.[19]

Further, the present status of the data-breach notification regime compounds the problems and costs associated with these breaches. Currently, when a company experiences a data breach it must look to the state law of every individual whose personal information was compromised in order to determine whether the injured individual must be notified of the breach and, if so, within

---

13. *Id.* Phishing scams are "email messages, websites, and phone calls . . . designed to steal money." MICROSOFT, SAFETY & SECURITY CENTER: HOW TO RECOGNIZE PHISHING EMAIL MESSAGES, LINKS, OR PHONE CALLS, http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx (last visited Oct. 27, 2014). Such scams are facilitated when a cybercriminal contacts a person in order to "install malicious software on [their] computer or [to steal] personal information" from them through the use of false pretenses. *Id.* A common example of phishing scams are spam email messages convincing the receivers to click on a link or to download something onto their computer. *Id.* When this link is clicked, malicious software is installed onto the receiver's computer. *Id.*

14. *Data Breach Trends & Stats*, *supra* note 3 (citing VERIZON, 2012 DATA BREACH INVESTIGATION REPORT (2012)).

15. *Id.* (citing PONEMON INST. & SYMANTEC, *supra* note 4).

16. *Id.* (citing Gartner, *Gartner Top Predictions for 2012: Control Slips Away*, GARTNER (2011), http://www.gartner.com/it/content/1842100/1842125/december_21_top_predictions _ 2012dplummer.pdf?userId=35627490).

17. *See, e.g.*, Resnick v. AvMed, Inc., 693 F.3d 1317, 1322 (11th Cir. 2012) (former members of a health care plan brought various claims, including negligence and negligence per se, against AvMed after unencrypted laptops containing members' personal information were stolen from AvMed's corporate office); Krottner v. Starbucks Corp., 628 F.3d 1139, 1140–41 (9th Cir. 2010) (current and former Starbucks' employees brought a class action suit for negligence and breach of implied contract after a laptop was stolen containing 97,000 employees' personal information).

18. Hamilton, *supra* note 1. A data dump occurs when "[a] large amount of data [is] transferred from one system or location to another . . . ." *Data Dump Definition*, OXFORD DICTIONARIES, http://www.oxforddictionaries.com/us/definition/american_english/data-dump (last visited Sept. 29, 2014). Thus, an inadvertent data dump is a transfer of data in error or by accident.

19. Anne Flaherty, *Study Finds Online Privacy Concerns on the Rise*, YAHOO NEWS (Sept. 5, 2013, 1:42 AM), http://news.yahoo.com/study-finds-online-privacy-concerns-rise-040211677.html.

what timeframe.[20] When breaches involve thousands or even millions of people from many different states, compliance with each of these individual state-notification laws can be extremely challenging.[21]

Additionally, once an individual has been notified of a breach, she has limited legal recourse against the company or organization that exposed her personal information. Civil causes of action such as negligence, breach of fiduciary duty, and breach of contract have been adapted to cover data-breach claims without much success, and class action lawsuits by groups of victims can be difficult.[22] In part, this is because the law on standing and injury is not clear in data-breach cases due to a jurisdictional split within the federal appellate courts.[23] The First and Third Circuit Courts of Appeal, as well as the United States Supreme Court, have held that a risk of future harm alone is not enough to confer standing.[24] However, the Seventh and Ninth Circuits have held that standing may be conferred merely by the possible threat of identity theft.[25] Furthermore, even if standing is found, actual injury may not be. The First Circuit and other state and district courts have held that mitigation damages, such as replacement costs for bank cards, identity theft insurance, and ongoing credit monitoring, are a cognizable injury even where identity theft cannot be shown.[26] However, the Supreme Court has

---

20. Jeffrey Benzing, *Industry Backs Idea of Federal Data Breach Notification Law*, MAIN JUSTICE (July 18, 2013, 4:04 PM), http://www.mainjustice.com/2013/07/18/industry-backs-idea-of-federal-data-breach-notification-law/.

21. *Id.*

22. ZURICH, THE LIABILITY OF TECHNOLOGY COMPANIES FOR DATA BREACHES 4–5 (2010), *available at* https://www.advisen.com/downloads/Emerging_Cyber_Tech.pdf.

23. *Id.*

24. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1151 (2013); Katz v. Pershing, L.L.C., 672 F.3d 64, 78 (1st Cir. 2012); Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011); *see also In re* LinkedIn User Privacy Litig., 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013). In *Clapper*, the United States Supreme Court held that the "objectively reasonable likelihood" standard for injury-in-fact was not enough to show injury is "certainly impending." 133 S. Ct. at 1147; Rand McClellan, Clapper *and Data Breach Litigation*, JD SUPRA BUSINESS ADVISOR (Apr. 8, 2013), http://www.jdsupra.com/legalnews/clapper-and-data-breach-litigation-62495/. Thus, the Court implied that a plaintiff could not base his or her injury solely on costs incurred in order to prevent a future, hypothetical harm which may not occur. *Clapper*, 133 S. Ct. at 1147–50; *McClellan*, *supra*. Therefore, "an increased danger of identity theft" itself may not be enough to satisfy standing under *Clapper*. *Clapper*, *supra*. However, this case was brought under the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1881a (2012), so whether it will be confined to its facts (cases involving national security considerations) or broadly applied to data breach litigation is yet uncertain. *Id.*

25. Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010); Ruiz v. Gap, Inc., 380 F. App'x 689, 691 (9th Cir. 2010); Pisciotta v. Old Nat'l. Bancorp., 499 F.3d 629, 634 (7th Cir. 2007).

26. Anderson v. Hannaford Bros. Co., 659 F.3d 151, 162–67 (1st Cir. 2011); Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 864–66 (N.D. Cal. 2011); Kuhn v. Capital One Fin. Corp., 855 N.E.2d 790, 2006 WL 3007931, slip op. (Mass. App. Ct. 2006).

suggested, and the Ninth Circuit and the District Court for the Southern District of California have held, that actual identity theft must be demonstrated.[27]

In order to combat these problems the Data Security and Breach Notification Act of 2013 ("DSBNA")—a federal data-breach notification statute that would preempt the various state laws—was introduced in the Senate.[28] Under the DSBNA, companies would be required to take "reasonable measures" in order to protect data that contains customers' personal information.[29] But is this proposed national law, which mirrors existing state laws, the most effective way to protect consumers from data breaches? Will it create an incentive for companies to better protect data when it does not address legal remedies for individual victims or clarify whether standing and injury requirements can be met in instances where identity theft has not yet occurred or cannot be proven?

The answer to these questions is a resounding no. In order to be effective and to better prevent future breaches, a national law must create a stronger incentive than the proposed DSBNA for companies to protect consumers' sensitive personal information, perhaps by creating additional liability for companies that do not comply with set standards for storing and protecting data. Additionally, such a law may need to be coupled with more frequent usage of insurance policies and credit-monitoring services to protect both institutional and individual victims of breaches.

This Note will argue that the current data-breach notification laws should be replaced by a scheme that is more effective in preventing data breaches from occurring and that provides consumers with a remedy when a breach of their personal information does occur. Thus, this Note proceeds as follows: Part I explores the current status of both state and federal data-breach notification law within the United States. Part II considers what is wrong with the current statutory scheme, including the difficulty entities experience complying with various states' data-breach laws, the limited civil causes of action for victims of data breaches, the current jurisdictional split on the standing and injury requirements in data breach cases, and the challenges posed by the current scheme in consumer class action lawsuits. Part III analyzes possible ways to improve data-breach notification laws in the United States. Finally, Part IV evaluates these proposed solutions, and argues for either the adoption of a strong national statute that defines industry standards for protecting consumer data and increases liability for entities that do

---

27. *Clapper*, 133 S. Ct. at 1143; *see also supra* note 24 (for an explanation of why *Clapper* suggests that actual identity theft must be shown); Krottner v. Starbucks Corp., 406 F. App'x 129, 131 (9th Cir. 2010); In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 963 (S.D. Cal. 2012); *supra* note 24 (explaining why the Supreme Court's holding in *Clapper* currently has uncertain application in data-breach litigation).

28. Christin McMeley, *Federal Data Breach Legislation Introduced, but Will It Go Anywhere?*, JD SUPRA BUS. ADVISOR (June 25, 2013), http://www.jdsupra.com/legalnews/federal-data-breach-legislation-introduc-74498/. As of October 27, 2014, this bill was still being considered by the Senate Commerce, Science, and Transportation Committee. *S. 1193: Data Security and Breach Notification Act of 2013*, GOVTRACK (Sept. 11, 2013, 7:37 PM), http://www.govtrack.us/congress/bills/113/s1193.

29. McMeley, *supra* note 28.

not adequately implement these standards, or more expansive regulatory oversight that could accomplish both of these objectives through an administrative agency.

I. CURRENT DATA-BREACH LAW

At present, the United States is without a national comprehensive data breach scheme. Instead, there is a patchwork of national and state laws regarding privacy, data security, and notification in the event of a breach.[30] The current federal laws governing data breaches are: (1) the Computer Fraud and Abuse Act ("CFAA")[31]; (2) the Electronic Communications Privacy Act ("ECPA")[32]; (3) healthcare privacy laws, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[33]; and (4) financial data laws including the Gramm-Leach-Bliley Act of 1999 ("GLBA")[34] and Red Flags Rules of the Fair and Accurate Credit Transactions Act of 2003[35] ("FACT Act").[36] Other federal laws include the Health Information Technology for Economic and Clinical Health Act ("HITECH")[37], the Fair Credit Reporting Act[38], the Bank Secrecy Act[39], and the Children's Online Privacy Protection Act.[40] In addition to these federal laws, most states have a statutory scheme requiring companies to alert consumers when their personal information has been compromised.[41] Some states also have laws requiring more than mere notification, such as those that provide private causes of action or that require an attorney general or state agency also be notified of a breach.[42]

---

30. ZURICH, *supra* note 22, at 2.

31. 18 U.S.C. § 1030 (2008).

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

33. 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.). For an interesting discussion on how HIPAA was intended to be a privacy law only as an "afterthought," see Jana Sutton, *Of Information, Trust, and Ice Cream: A Recipe for A Different Perspective on the Privacy of Health Information*, 55 ARIZ. L. REV. 1171, 1177–78 (2013).

34. 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.).

35. Pub. L. No. 108-159, 117 Stat. 1952 (2003) (codified as amended in scattered sections of 15 U.S.C.).

36. ZURICH, *supra* note 22, at 3.

37. Pub. L. No. 111-5, §§ 13001-424, 123 Stat. 226 (2009).

38. Pub. L. No. 91-508, Title VI, 84 Stat. 1114 (1970) (codified as amended at 15 U.S.C. §§ 1681-1681x).

39. Pub. L. No. 91-508, 84 Stat. 1114-2 (1970) (codified as amended in scattered sections of 12 U.S.C. and 31 U.S.C.).

40. 15 U.S.C. §§ 6501-6506 (1998). ZURICH, *supra* note 22, at 3. Due to the amount of federal laws listed above, only those relevant to this Note will be discussed in Section A of this Part.

41. *Id*.

42. BAKERHOSTETLER, DATA BREACH CHARTS 11–15, (2014), http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.

A. National Laws

Federally, there are various institutionally applicable or narrowly tailored privacy and data security laws, none of which relate directly to data-breach notification for consumers. For example, in response to the emergence of computers and the use of technology, Congress passed the CFAA[43] in 1984. The CFAA was intended to criminalize hacking[44] by making it a crime to access, obtain information from, or use or transmit something to a computer in certain instances.[45] However, the CFAA also created a private civil cause of action, which may be applicable to data security breaches in two limited circumstances.[46] These include instances wherein 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.[47] And, because a "protected computer" includes any computer "which is used in or affect[s] interstate or foreign commerce or communication"[48]—meaning any computer with internet access—this act appears to have great potential in providing a remedy to consumer victims of a data breach. However, the CFAA has yet to be effectual for this purpose.[49] First, the CFAA has limited application against corporations who experience a security breach because an action may not be brought for "the negligent design or manufacture of computer hardware, computer software, or firmware."[50] Furthermore, in two cases where the

---

43. The CFAA is codified at 18 U.S.C. § 1030 (2012).

44. *Computer Fraud and Abuse Act Reform*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/cfaa (last visited Oct. 27, 2014).

45. The CFAA makes it a crime to, without authorization or by exceeding authorized access: (1) knowingly access a computer in order to obtain classified information; (2) obtain financial information from a financial institution, credit reporting agency, or the government, or obtain information involving conduct relating to interstate or foreign commerce (copying or removal of the information is not required); (3) access computers used by the government (causing damage or stealing property is not required); (4) use computers in any manner to defraud a person of their property (this requires access of a computer used by the United States or a financial institution without authorization to obtain anything with a value of more than $5,000); (5) knowingly transmit a program, information, code, or command with the purpose of intentionally damaging a protected computer; (6) share a password or other similar information which would allow unauthorized access to a protected computer; or (7) transmit a communication of a threat to damage a protected computer for the purpose of extortion or obtaining money. 1 Law of the Internet (MB) Ch. 7, § 2 (Dec. 2013); 18 U.S.C. § 1030(a)(1)–(7); 18 U.S.C. § 1030(e)(2); DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 4 (2010), http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf. The CFAA also covers conspiracies and attempts to violate its provisions. 18 U.S.C. § 1030(b). In addition, any violation of the CFAA is punishable by criminal sanctions, and sentencing for convictions is based on the amount of damage caused. Law of the Internet, *supra*; 18 U.S.C. § 1030(c).

46. 18 U.S.C. § 1030(g); P. Scott Ritchie et al., *Security Breach Cases Under Federal Law: A Brief Analysis*, CLAUSEN MILLER PC (Sept. 2013), http://www.clausen.com/index.cfm/fa/firm_pub.article/article/5e850e7a-9245-44b6-b87a-ca722a622d10/Security_Breach_Cases_Under_Federal_Law_A_Brief_Analysis.cfm.

47. 18 U.S.C. § 1030(c)(4)(A)(i); Ritchie, *supra* note 46.

48. 18 U.S.C. § 1030(e)(2); DEP'T OF JUSTICE, *supra* note 45.

49. *See* Ritchie, *supra* note 46.

50. *Id.*; 18 U.S.C.A. § 1030(g).

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.[51] Thus, although the CFAA may have some application to data security breaches, it has yet to be successfully invoked by a consumer.

The ECPA is a federal privacy law, passed in 1986, meant to protect individuals from government eavesdropping.[52] The ECPA makes it illegal for people to intercept wire, oral, or electronic communications, unless they are a law enforcement agency with judicial approval.[53] The ECPA also regulates the privacy of and government access to stored electronic communications, as well as the government's use of pen registers and "trap and trace" devices.[54] Thus, the ECPA was intended to "provid[e] greater privacy protection" for individuals from government intrusion,[55] not to notify consumers that their personal information has been breached or to provide them with a remedy for such.

One of the largest federal privacy and data security laws, HIPAA, protects "individually identifiable *health* information" only.[56] To comply with Sections 261–264 of HIPAA, the U.S. Department of Health and Human Services ("DHHS") promulgated the Standards for Privacy of Individually Identifiable Health Information ("Standards").[57] The Standards protect information relating to:

---

51. Ritchie, *supra* note 46. These cases include the following: *In re Google Android Consumer Priv. Litig.*, 2013 WL 1283236 (N.D. Cal. Mar. 26, 2013) (plaintiffs claimed Google used code within its applications to collect personally identifiable information, which was used for marketing and research purposes, without the consent or knowledge of the plaintiffs); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012) (plaintiffs claimed Apple's use of iDevice to store information on their location violated the CFAA). *Id.*

52. CHARLES DOYLE, CONG. RESEARCH SERV., R41733, PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 1, 6 (2012), *available at* http://fas.org/sgp/crs/misc/R41733.pdf.

53. *Id.* at 1; 18 U.S.C. §§ 2510-2522 (2002).

54. DOYLE, *supra* note 52, at 1; 18 U.S.C. §§ 2701–2712 (2001); 18 U.S.C. §§ 3121–3127 (2001). Pen registers are devices used by law enforcement to record the phone numbers that a person dials and "trap and trace" devices are used to record the phone numbers of incoming callers. ELECTRONIC FRONTIER FOUNDATION, *"Pen Registers" and "Trap and Trace Devices,"* THE SURVEILLANCE SELF-DEFENSE PROJECT, https://ssd.eff.org/wire/govt/pen-registers (last visited Apr. 16, 2014). Used together, these devices can provide information on incoming and outgoing calls including the specific time calls were made, the length of a call, and if a call was answered. *Id.*

55. U.S. Dep't of Justice, *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22*, JUST. INFO. SHARING, https://it.ojp.gov/default.aspx?area=privacy&page=1285 (last updated July 30, 2013).

56. Pub. L. No. 104-191, 110 Stat. 1936 (1996); U.S. DEP'T OF HEALTH & HUMAN SERVS., HEALTH INFORMATION PRIVACY, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html (last visited Oct. 27, 2014) (emphasis added).

57. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html (last visited Oct. 13, 2013).

> [T]he 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.[58]

The Office for Civil Rights, a division within the DHHS, may impose a civil monetary penalty of $50,000 or more upon an entity for each violation of the Standards.[59] In addition, criminal prosecution may be an accessible remedy depending on the specific violation.[60] However, HIPAA does not provide for a private cause of action[61] and does not relate to personally identifiable information other than individually identifiable health information.

Another federal statute, the GLBA, was passed by Congress in 1999 in order to regulate how financial institutions handle, store, and disclose individuals' personal financial information.[62] The GLBA, therefore, is applicable to financial institutions only and 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.[63] Financial institutions that violate the GLBA face civil penalties of up to $100,000 per violation and civil penalties of up to $10,000 levied against the officers and directors of the institution per violation.[64] In addition, criminal penalties are possible for anyone who knowingly and intentionally obtains customer information through the use of false pretenses—including fines, up to five years in prison, or both.[65]

Finally, the FACT Act of 2003 amended the Fair Credit Reporting Act[66] to better prevent identity theft and, in addition, to provide individual consumers

---

58. *Id.* (citing 45 C.F.R. § 160.103).

59. *Id.*

60. *Id.*

61. Edward Vishnevetsky, *Can A HIPAA Violation Give Rise to a Private Cause of Action?*, HEALTHCARE DAILY (May 27, 2014), http://healthcare.dmagazine.com/2014/05/27/can-a-hipaa-violation-give-rise-to-a-private-cause-of-action/.

62. Margaret Rouse, *Gramm-Leach-Bliley Act (GLBA)*, TECHTARGET, http://searchcio.techtarget.com/definition/Gramm-Leach-Bliley-Act (last visited Oct. 27, 2014).

63. *Id.*

64. 15 U.S.C. § 6821 (1999); ECORA, PRACTICAL GUIDE TO UNDERSTANDING AND COMPLYING WITH THE GRAMM-LEACH-BLILEY ACT 3 (2007), *available at* http://www.ecora.com/Ecora/ whitepapers/IDRS_GLBA.pdf.

65. 15 U.S.C. § 6823; PRACTICAL GUIDE TO UNDERSTANDING AND COMPLYING WITH THE GRAMM-LEACH-BLILEY ACT, *supra* note 64, at 3. Fines imposed as criminal penalties under the GLBA are to be done in accordance with title 15 of the United States Code. 15 U.S.C. § 6823(a). Therefore, fines will vary based on whether the offense is a felony or misdemeanor, whether the offense resulted in death, whether the offense resulted in a pecuniary gain to the defendant or loss to another, and in accordance with other various listed factors. 15 U.S.C. §§ 3571, 3572(a) (1996).

66. 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–

better access to their credit reports.[67] In 2007 the Federal Trade Commission ("FTC") passed the Red Flags Rules to implement a provision in the FACT Act of 2003 that addresses the "duties of creditors, card issuers and users of consumer reports[,]" to help prevent identity theft.[68] This requires certain institutions to "identify and respond to account activities that are possible indicators ('red flags') of identity theft . . . ."[69] Thus, the FACT Act is statutory law regarding credit reporting, and does not have broad application outside of that specific arena.[70]

In sum, although there is an existing patchwork of federal laws relating to consumer data and privacy already in existence, these laws tend to be narrowly tailored to specific kinds of data in specific instances or industries. And, even when they do have potential broad application to data breaches, such as the CFAA, consumers have not been successful in bringing claims under them. Thus, there is no broad, overarching federal legislation that addresses the use or storage of data containing personal consumer information in general across all industries.

B. State Laws

Currently, 47 states have data-breach notification laws.[71] These laws require that, when certain conditions are present in a data breach, companies inform consumers that their personal information has been or may have been exposed.[72] Only Alabama, New Mexico, and South Dakota do not currently have notification laws.[73]

However, although most states have data-breach notification laws already in place, these laws differ greatly from each other in significant ways, creating

---

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).

67. THE CATHOLIC UNIV. OF AMERICA, OFFICE OF GENERAL COUNSEL: SUMMARY OF FEDERAL LAWS, http://counsel.cua.edu/fedlaw/fcra.cfm (last visited Oct. 13, 2013).

68. NINA LAVOIE, IDENTITY THEFT RED FLAGS AND ADDRESS DISCREPANCIES UNDER THE FCRA 1 (2008), *available at* http://www.nacua.org/documents/FACTA_General Summary_091508.pdf.

69. Yoon-Young Lee, *FACT Act "Red Flag" Rules*, WILMERHALE (Sept. 2, 2008), http://www.wilmerhale.com/pages/publicationsandNewsDetail.aspx?NewsPubId= 91 356.

70. *Fact Sheet 6a: Facts on FACTA, the Fair and Accurate Credit Transactions Act*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/facts-facta-fair-and-accurate-credit-transactions-act#10 (last visited Oct. 27, 2014).

71. *State Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGISLATURES (Sept. 3, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. A chart listing each of these states and their various statutory provisions regarding data-breach notification may be found at DATA BREACH CHARTS, *supra* note 42.

72. *See* GINA STEVENS, CONG. RESEARCH SERV., R42475, DATA SECURITY BREACH NOTIFICATION LAWS 4 (2012), *available at* http://fas.org/sgp/crs/misc/R42475.pdf.

73. *State Security Breach Notification Laws*, *supra* note 71.

compliance issues for large national entities with nationwide customer bases. The only apparent commonality with these various state notification laws is that most require consumer notification only when the compromised data was not encrypted, or when the encryption key was also compromised.[74] One of the ways state laws differ significantly from one another is in their definition of what constitutes "personal information."[75] Typically, personal information includes:

> (a) [a] first name or first initial 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) [a] 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.[76]

However, 25 states define personal information more broadly,[77] including passwords, PIN numbers, access codes for financial accounts,[78] medical information,[79] health insurance information,[80] routing numbers in combination with the necessary access code or password,[81] unique biometric data (such as fingerprints),[82] and individual Taxpayer Identification Numbers.[83]

In addition, only seven states provide a specific time frame for notification to consumers.[84] These timeframes range from 5–45 days after the incident is discovered.[85] However, five of these seven states allow for the delay of statutory timeframes pursuant to the legitimate needs of law enforcement officials.[86]

---

74. DATA BREACH CHARTS, *supra* note 42, at 15–18. This provision is called an "encrypted data safe harbor." 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).

75. *See* DATA BREACH CHARTS, *supra* note 42.

76. ARIZ. REV. STAT. ANN. § 44-7501 (2013). Publically available information is not included in the definition of "personal information." *Id.*

77. DATA BREACH CHARTS, *supra* note 42, at 2–6.

78. *See, e.g.*, ALASKA STAT. § 45.48.090 (2013).

79. *See, e.g.*, ARK. CODE ANN. § 4-110-103 (2014).

80. *See, e.g.*, MO. REV. STAT. § 407.1500 (2014).

81. *See, e.g.*, *id.*

82. *See, e.g.*, IOWA CODE ANN. § 715C.1 (2013).

83. *See, e.g.*, MD. CODE ANN., COM. LAW § 14-3501 (2013).

84. DATA BREACH CHARTS, *supra* note 42, at 13–14. These states include California, Connecticut, Florida, Maine, Ohio, Vermont, and Wisconsin. *Id.*

85. *Id.*

86. *Id.* These states include Florida, Maine, Ohio, Vermont, and Wisconsin. *Id.* Delay for the legitimate needs of law enforcement may include a criminal investigation wherein notification could compromise that investigation. *See, e.g.*, ME. REV. STAT. tit. 10, § 1348(3) (2009). The delay imposed on the statutory timeframe, therefore, may be "for a specified period that the law enforcement agency determines is reasonably necessary." *See, e.g.*, FLA. STAT. § 501.171(4)(b) (2014).

Further complicating the issue is that, while seven states require notification within a certain number of days, some states do not allow a notification to be given until an analysis of the effects of the breach is conducted. For example, 41 states require analysis of a breach's risk-of-harm as a prerequisite for determining whether notification is required.[87] Thus, entities experiencing a data breach with consumers in states with both types of legislation must somehow comply with both of these requirements—notifying those in states with specific timelines for notification (some as short as five days) within the required time, while not notifying others until a risk-of-harm analysis is completed. This may create an enormous burden for large national entities to distinguish between thousands or even millions of customers and to determine what the entity must legally do to notify or not notify each.

Other differences in various state notification laws include, for example, that only 14 states provide a private cause of action for persons injured by a breach,[88] 7 states have notification laws which also apply to a breach involving paper documents,[89] and 21 states require that an attorney general or state agency be notified of a data breach.[90] Thus, it is clear that, although most states do currently have data-breach notification laws, these laws differ immensely. Compliance under one state's law may not equal compliance under another's, causing confusion for entities who have experienced a breach and are attempting, in good faith, to comply with each state's laws.

II. PROBLEMS WITH THE CURRENT LAW

Currently, there are many issues with the existing data-breach regime which should be improved in order to better protect consumers and allow for easier compliance by entities experiencing large-scale data breaches. First, because data-breach notification laws vary from state to state, compliance with each may be difficult in large, nationwide data-breach incidents.[91] Second, constitutional standing and injury requirements make it extremely challenging for consumers to bring a claim against a company whose consumer data has been compromised.[92] This challenge is further complicated by the uncertainty created by various constitutional requirements for standing and injury within each of the federal circuits.[93] Third, the difficulty of bringing a class action suit with other consumer victims[94] and the inapplicability of many currently existing civil causes of action to data breaches further complicate the ability of consumers to hold corporations liable for breaches exposing their personal information.[95] Thus, these three issues with the current law, taken together, render data-breach notification laws

87. DATA BREACH CHARTS, *supra* note 42, at 7–11.

88. *Id.* at 14–15. Or for the data collector who was harmed by the person unlawfully obtaining his or her records. *Id.*

89. *Id.* at 18–19.

90. *Id.* at 11–13.

91. *See* Benzing, *supra* note 20; *infra* Part II.A.

92. *See infra* Part II.C.

93. *See infra* Part II.C.

94. *See infra* Part II.D.

95. *See infra* Part II.B.

ineffective in preventing data breaches from occurring and in providing consumers with a remedy when they do occur.

A. Compliance and Other Issues with the Various State Laws

The differences in current state data-breach notification laws should be resolved in order to make compliance less burdensome and costly for large national entities that have customers in multiple states. Differences in state laws create confusion for both companies and consumers, and provide for situations in which consumers may fall through the cracks. Resolving these differences is necessary because the variations in state laws creates complexity for national companies in determining which laws to comply with and how to do so.[96] This is because many of these laws vary dramatically in: what constitutes "personal information"; notification exemptions; timelines in which notification must take place; procedures for notification; and penalties for failure to comply with the statute.[97] For example, some states require a risk-of-harm analysis to determine whether the breach "is likely to cause substantial economic loss to an individual,"[98] or whether "an illegal use of personal information has occurred, or is reasonably likely to occur"[99] before notification will even be required.[100] This, coupled with other differences—such as the difference in notification deadlines varying from 5 days, to 45 days, to "the most expedient time possible"—can lead to extreme confusion and might prevent some consumers from receiving notification at all.[101]

Another problem with the current notification scheme is that, rather than being proactive in preventing data breaches, these laws are reactive by only requiring notification *after* a breach.[102] The main purpose of these state laws is to "allow consumers to protect themselves against identity theft" and to "mitigate damages resulting" from data breaches.[103] As it stands, the notification scheme does little to incentivize the development of more efficient methods for protecting sensitive consumer data. While it is possible that bad publicity resulting from a breach may incentivize some companies to take better precautions against future breaches, most companies only become better at notifying consumers that their data has been compromised when it is already too late.[104]

Furthermore, though it might be argued that notification laws create incentives for companies to avoid data breaches by making the cleanup costly and burdensome, some companies—especially retailers—actually benefit more from collecting consumer data than they do from protecting it.[105] Thus, the rise in

---

96. *See* Joerling, *supra* note 74, at 483; Benzing, *supra* note 20.
97. *See supra* Part I.B; Joerling, *supra* note 74, at 485; Benzing, *supra* note 20.
98. ARIZ. REV. STAT. § 44-7501 (2008).
99. HAW. REV. STAT. ANN. § 487N-1 (2009).
100. Joerling, *supra* note 74, at 474–76.
101. *Id.* at 477, 483; *see supra* Part I.B.
102. Joerling, *supra* note 74, at 483–84.
103. *Id.* at 471.
104. *Id.* at 484.
105. Jose Pagliery, *Why Retailers Aren't Protecting You From Hackers*, CNN MONEY (Feb. 18, 2014, 6:56 AM), http://money.cnn.com/2014/02/18/technology/

corporate data breaches over the past decade—notwithstanding the overall increase in notification laws—supports the argument that the current state laws are not effective enough to prevent data breaches.[106]

It is clear that, although these statutes were a step in the right direction when enacted, they are not effective enough in preventing data breaches or protecting private consumer information. Instead, they are adding to the confusion surrounding the current data-breach regime. These laws need to be made more concise and clear in order to facilitate compliance and better protect consumers.

B. Limited Civil Causes of Action

When a company experiences a data breach, the recourse available to an injured consumer is limited. As indicated above,[107] only 14 states' data-breach notification laws provide various private causes of action.[108] In states that do not provide such a remedy, or in states that provide only private causes of action for the injured company,[109] consumers must look to other theories of recovery such as breach of contract, breach of implied contract, breach of fiduciary duty, negligence, public disclosure of private facts, state consumer protection laws, and emotional distress.[110] However, these claims are typically successful only when the company has not provided timely notification.[111]

---

security/retail-hack/ (explaining that if credit card systems are improved in order to better protect data from hackers, then retailers will no longer have access to information used for marketing purposes, which increase retailer returns by as much as 60%; and furthermore, the cost to banks and retailers in implementing more secure technology is estimated to cost upwards of $8 billion).

106. Joerling, *supra* note 74, at 484.

107. *See supra* Part I.B.

108. DATA BREACH CHARTS, *supra* note 42, at 14–15; *see, e.g.*, CAL. CIV. CODE § 1798.84(b) (2010).

109. DATA BREACH CHARTS, *supra* note 42, at 14–15; *see, e.g.*, NEV. REV. STAT. ANN. § 603A.900 (2012).

110. IAN C. BALLON, E-COMMERCE & INTERNET LAW 27.07 (2d ed. 2013) (*available at* WestlawNext); ZURICH, *supra* note 22, at 4. Claims have also been brought by consumers under the federal Stored Communications Act, 18 U.S.C.A. §§ 2701–2711 (2009), but have not been successful due to the statute's limitations, which require that disclosure of data knowingly be made, and that its provisions are limited to electronic communication services ("ECS") and remote computing services ("RCS"). Ballon, *supra*; *see, e.g.*, Worix v. MedAssets, Inc., 857 F. Supp. 2d 699, 701–03, 707 (N.D. Ill. 2012) (dismissing plaintiff's claims without prejudice because section 2702(a)(1)–(2) requires that the plaintiff show the defendant's disclosure was knowingly made); *In re* Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 523–24 (N.D. Ill. 2011) (citing 18 U.S.C. § 2711(2)) (holding that Michaels was not an ECS or RCS provider; defining ECS providers as those who provide internet or phone services through which data is transmitted and RCS providers as those who provide public computer or processing services by means of an ECS) .

111. 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

One reason for the limited success of existing causes of action, as applied to data breaches, is attributable to the economic loss doctrine, which bars recovery in tort actions where only purely economic losses are asserted.[112] In *In re Michaels Stores PIN Pad Litigation*, the United States District Court for the Northern District of Illinois held that claims of negligence and negligence per se could not survive dismissal when personal injury or property damages could not be demonstrated—only increased risk of identity theft and economic loss damages were alleged.[113] Similarly, in *Rowe v. UniCare Life and Health Insurance Co.*, the same court 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 exposure of his information to the public."[114]

Additionally, claims for breach of fiduciary duty tend to fail in this context because there is no fiduciary obligation between the consumer and the breaching company.[115] For example, in *Andersen v. Hannaford Brothers Co.*, the First Circuit dismissed a 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.'"[116] However, 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.[117] Thus, *Andersen* makes it difficult for a breach of fiduciary duty claim to be successful in the data-breach context.

On the other hand, breach-of-implied-contract claims have shown some success in being adapted to cover data breaches. In *Anderson*, the First Circuit reversed a district court's dismissal of such a claim, stating that a reasonable jury could conclude that an implied contract exists between consumers and companies they purchase from.[118] The court stated this flowed from an inference that 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."[119] Thus, a fact-finder could determine that "an implicit agreement to safeguard . . . data is necessary to effectuate [a] contract" between a customer and

---

Michaels did not timely notify its customers of the data breach in its reasoning for upholding both claims).

112. *In re* Michaels Stores Pin Pad Litig., 830 F. Supp. 2d at 528; Ballon, *supra* note 110.

113. *In re* Michaels Stores Pin Pad Litig., 830 F. Supp. 2d at 526, 531. For additional information on the economic loss doctrine, see William A. Bianco, *The Economic Loss Rule: Some Practical Consequences of the Distinction Between Contractual Duties and Other Legal Duties*, URS CLAIMS AND DISPUTE RESOLUTION GROUP (2007), *available at* http://www.dgslaw.com/images/materials/Bianco_EconomicRule.pdf.

114. Rowe v. UniCare Life & Health Ins. Co., No. 09-C-2286, 2010 WL 86391, at *6 (N.D. Ill. Jan. 5, 2010); Ballon, *supra* note 110.

115. Ballon, *supra* note 110.

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

117. *Id.* at 158.

118. *Id.* at 159.

119. *Id.*

a retailer.[120] However, this remedy is likely limited due to the First Circuit's implication that a company taking reasonable measures to protect customer data would probably not be liable when a breach occurs.[121]

Finally, as illustrated below, another principle reason that civil causes of action in data-breach cases are rarely successful is the difficulty consumer data-breach victims have in meeting the standing and injury requirements.[122]

C. The Standing and Injury Circuit Split

Arguably, one of the most complicated aspects of the current data breach regime is the circuit split regarding the plaintiff's burden to establish standing and injury in data breach cases.[123] This split creates confusion for potential consumer plaintiffs who are the victims of data breaches, in addition to making success difficult unless the plaintiff can establish a nexus between the data breach and the resulting harm. For example, where it is uncertain whether the plaintiff's personal information was actually taken in a data breach or no resulting harm (other than mitigation costs in the prevention of future identity theft) can be shown, meeting the requirements of standing and injury may be extremely difficult. What these cases do not take into account is the damage which may be caused in the future once personal information has gotten into the wrong hands or the difficulty in demonstrating that a specific data breach was the precipitator of a specific instance of identity theft. Thus, a nationwide, statutory legal remedy for consumers should be created in order to eliminate this circuit split and clarify standing and injury in data-breach suits.

---

120. *Id.*

121. *Id.*

122. Madden, *supra* note 111, at 29–31.

123. Article III of the Constitution states that a plaintiff must establish standing during the pleading stage of a case. Paul Pittman, *Consumer Data Privacy and Data Breach Claims Haven't Had a Leg to Stand on, But Support May Be on the Way*, JD SUPRA BUS. ADVISOR (April 8, 2013), http://www.jdsupra.com/legalnews/consumer-data-privacy-and-data-breach-cl-14508/; 13B Fed. Prac. & Proc. Juris. § 3532.1, ¶ 10 (3d ed.). This, in part, requires that a plaintiff allege injury-in-fact—a "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013); Pittman, *supra*. For additional discussion of the Article III standing requirement, see *Clapper*, 133 S. Ct. at 1146–47. Ripeness, another Article III requirement, "assumes that an asserted injury is sufficient to support standing, but asks whether the injury is too contingent or remote to support present adjudication." 13B Fed. Prac. & Proc. Juris. § 3532.1, ¶ 10 (3d ed.). In other words, "ripeness asks whether there yet is any need for the court to act." *Id.* Thus, a plaintiff must show an actual injury when stating a claim for which the court may grant relief. Pittman, *supra* note 123. And, most importantly, because a plaintiff must meet all three of the Article III requirements, it is possible for courts to find that the standing requirement, but not the injury requirement, which is comprised of all three Article III requirements, has been met in certain cases. For an overview of Article III's requirements and their impact on injury, see Fed. Prac. & Proc. Juris. § 3532.1 (3d ed.). *See also*, Krottner v. Starbucks Corp., 406 F. App'x 129 (9th Cir. 2010); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., MDL No. 11MD2258, 2012 WL 4849054 (S.D. Cal. Oct. 11, 2012).

1. Demonstrating the Data Breach and the Identity Theft Nexus

Standing and injury exist only in rare cases where a "nexus between the data breach and the identity theft" can be established.[124] For example, in *Resnick v. AvMed*, the Eleventh Circuit held that standing and injury had been shown where the private, unencrypted information stolen during a data breach was used 10–14 months later to steal the identity of the data breach victims.[125] Thus, the plaintiffs' injury was fairly traceable to the defendant's data breach, establishing injury in fact, and making monetary damages from the resulting identity theft a cognizable injury.[126] The plaintiffs also presented evidence that they had taken "substantial precautions" to prevent identity theft and that, prior to the breach at issue, had never had their identities stolen.[127]

However, demonstrating such a "nexus" between a plaintiff's injury and a defendant's data breach may be an insurmountable hurdle for many plaintiffs, as it may be impossible to show that information taken in a specific data breach was the same information later used to steal an identity.[128] This is especially true because breaches of similar personal information occur frequently, and many are not discovered until months or even years later.[129] For example, if a person is the victim of two or more data breaches in which similar personal information is stolen and that information is not used until years later to harm her, it may be difficult for the victim to demonstrate which breach was the source of the information used.

a. Standing Based on Mere Threat of Identity Theft

In cases where no nexus can be shown, the Seventh and Ninth Circuits have held that the mere threat of identity theft may be enough to satisfy the standing requirement when it can be shown that a data breach has occurred and that the plaintiff's personal information was stolen. For instance, in *Pisciotta v. Old National Bancorp*, the Seventh Circuit held that injury in fact could be demonstrated where the plaintiffs' personal information had been stolen during a malicious breach of the defendant's website-hosting facility, but had not yet been used to harm them.[130] No financial loss or other harm was pled.[131]

In addition, the Ninth Circuit held in *Krottner v. Starbucks Corp.* that "[i]f a plaintiff faces 'a credible threat of harm[,]' . . . and that harm is 'both real and immediate, not conjectural or hypothetical,' . . . the plaintiff has met the injury-in-fact requirement for standing under Article III."[132] In *Krottner*, that harm was demonstrated when the plaintiff's laptop—which contained unencrypted

124. Resnick v. AvMed, Inc., 693 F.3d 1317, 1330 (11th Cir. 2012).
125. *Id.* at 1326–27.
126. *Id.* at 1324.
127. *Id.* at 1326.
128. *See* Pittman, *supra* note 123.
129. VERIZON, *supra* note 1, at 51–52; *see supra* notes 1–4.
130. 499 F.3d 629, 634 (7th Cir. 2009).
131. *Id.* at 632.
132. 628 F.3d 1139, 1143 (9th Cir. 2010) (internal citations omitted).

personal data—was stolen.[133] The court went on to state that the conjectural and hypothetical elements of the test applied to whether *the actual breach had occurred* and that if the claim was based on the possibility of the breach in the future, then standing would not have been found.[134] Similarly, in *Ruiz v. Gap, Inc.*, the Ninth Circuit held that the plaintiff had standing where a laptop containing the plaintiff's social security number was stolen.[135] There, because the plaintiff could allege that he "was at a greater risk of identity theft[,]" his injury was not merely speculative and was enough to confer standing.[136]

b. Standing Based on Certainly Pending Injury

Unlike the Seventh and Ninth Circuits, the Supreme Court, First Circuit, and Third Circuit have suggested that an increased risk of future harm from a data breach is not enough to confer standing when it is uncertain whether a plaintiff's information has actually been stolen. In *Clapper v. Amnesty Int'l USA*, the Supreme Court held that when a plaintiff's "theory of standing . . . relies on a highly attenuated chain of possibilities, [it] does not satisfy the requirement that threatened injury must be certainly impending."[137] There, the plaintiffs brought claims under the Foreign Intelligence Surveillance Act of 1978 ("FISA")[138] and based their injury on the possibility that the federal government would target and intercept their communications with foreign persons using FISA as their authority.[139] The Court determined that the plaintiffs' injury was too attenuated because there was no evidence that the government would target such communications or intercept them by invoking its authority under FISA.[140] The Court stated that plaintiffs should not be allowed to "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[141]

In addition, the Court stated that it has "repeatedly reiterated that 'threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient."[142] Thus, although *Clapper* was not decided in the context of data breach, the Court's reasoning suggests that alleging an increased danger of identity theft alone may be an injury too distant and hypothetical.[143] Therefore, proof of costs incurred to prevent the possibility of future identity theft, without more, may be insufficient to confer standing when it is unclear whether a data breach has actually occurred or whether

133. *Id.* at 1140–41.
134. *Id.* at 1142.
135. Ruiz v. Gap, Inc., 380 F. App'x 689, 690 (9th Cir. 2010).
136. *Id.* at 691.
137. 133 S. Ct. 1138, 1148 (2013).
138. 50 U.S.C. § 1881a (2008).
139. *Clapper*, 133 S. Ct. at 1143, 1148.
140. *Id.* at 1148–50.
141. *Id.* at 1151.
142. *Id.* at 1147 (emphasis and alteration in original) (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).
143. McClellan, *supra* note 24.

someone's data was actually taken.[144] However, it is uncertain how *Clapper* will be applied and interpreted in the context of data-breach litigation in the future.[145]

Unlike *Clapper*, the decisions of the First and Third Circuits were specifically made in the context of data-breach litigation. In *Reilly v. Ceridian Corporation*, the Third Circuit held that "allegations of hypothetical, future injury are insufficient to establish standing."[146] There, employees of companies who used the defendant–company to process their payroll were notified that a hacker might have accessed their personal information—but it was not clear whether the hacker actually read or copied the information.[147] The plaintiffs alleged an increased risk of identity theft, which the court found to be too attenuated, as it was "entirely speculative" and not "certainly impending."[148] In addition, the court stated that the expenses incurred by the plaintiffs in attempting to protect themselves from possible identity theft were "no more 'actual' injuries" than the increased risk of identity theft, and therefore not a "result of any *actual* injury."[149]

Moreover, in *Katz v. Pershing, L.L.C.*, the First Circuit held that a plaintiff did not have standing where the plaintiff could not point to a specific data breach that exposed the plaintiff's personal information.[150] There, the plaintiff alleged that because the defendant's website did not adequately protect her personal information, "a 'massive number of breaches of security [] ha[d] invariably occurred' and that, as a result, some level of unauthorized access must have transpired, thereby exposing some . . . non-public personal information . . . ."[151] However, the plaintiff did not cite to any specific instances when *her* nonpublic personal information was accessed.[152] Therefore, the court held that, without an "identified breach," there was no Article III standing.[153]

2. Finding Standing, But Not Injury

Furthermore, even if a data-breach victim meets the standing requirements, he or she must also satisfy the injury requirements, or his or her case may be dismissed.[154] In this context, there is a circuit split regarding whether mitigation costs after a data breach are enough to demonstrate an actual injury, or if a plaintiff must plead damages from an actual identity theft injury.

a. Mitigation Costs to Establish Actual Injury

---

144. *Id.*

145. *Id.* See McClellan, *supra* note 24 for an additional discussion about how *Clapper* may be applied broadly or limited only to FISA in future litigation. Predicting the application of *Clapper* is beyond the scope of this Note.

146. 664 F.3d 38, 42 (3d Cir. 2011).

147. *Id.* at 40.

148. *Id.* at 40, 42–43.

149. *Id.* at 46.

150. 672 F.3d 64, 79 (1st Cir. 2012).

151. *Id.* at 70, 79.

152. *Id.* at 79.

153. *Id.*

154. Pittman, *supra* note 123.

The First Circuit and the Massachusetts Court of Appeals have held that the costs of preventing identity theft following a data breach are enough to establish an actual injury, even when identity theft has not yet occurred.[155] For example, in *Anderson v. Hannaford Brothers Co.*, after the plaintiff shopped at several of the defendant's grocery stores, the defendant's electronic payment-process system was hacked, compromising consumers' debit card information.[156] The First Circuit held that, under Maine law, the costs associated with identity theft insurance and replacement debits cards were recoverable under a theory of negligence if they are "reasonably foreseeable under the circumstances," and under a breach of contract theory, "so long as they are reasonable."[157] However, lost reward points, lost opportunities arising from such points, and fees for pre-authorization charges, were too attenuated as they stemmed from a third party's reaction to the breach and not from the breach itself.[158]

Similarly, in *Kuhn v. Capital One Financial Corp.* the Massachusetts Court of Appeals reversed a grant of summary judgment in favor of a credit card company, finding that "one 'whose legally protected interests have been endangered by the tortious conduct of another is entitled to recover for expenditures reasonably made or harm suffered in a reasonable effort to avert the harm threatened.'"[159] In *Kuhn*, while the fraudulent accounts opened in the plaintiff's name did not cause her monetary damages, the time she spent calling credit rating agencies in order to close the accounts and prevent future harm was sufficient to establish actual damages.[160]

b. Requirement of Identity Theft to Establish Actual Injury

On the other hand, the Supreme Court has implied, and district and appellate courts in the Ninth Circuit have held, that actual identity theft itself is required in order to satisfy the actual injury requirement.[161] As previously stated, though *Clapper* was not specifically in the context of data-breach litigation, its holding might be applied to the doctrine in the future.[162] In *Clapper*, the Supreme Court stated that a plaintiff "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending[,]" implying that in a data-breach context mitigation costs spent to prevent future identity theft would not satisfy the injury requirement when no actual identity theft has occurred.[163]

---

155. Anderson v. Hannaford Brothers Co., 659 F.3d 151 (1st Cir. 2011); Kuhn v. Capital One Fin. Corp., 855 N.E.2d 790 (Mass. App. Ct. 2006).

156. *Anderson*, 659 F.3d at 153.

157. *Id.* at 162, 167.

158. *Id.* at 167.

159. *Kuhn*, 855 N.E.2d at *3 (quoting RESTATEMENT (SECOND) OF TORTS § 919 (1979)).

160. *Id.*

161. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013); Krottner v. Starbucks Corp., 406 F. App'x 129 (9th Cir. 2010); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 963 (S.D. Cal. 2012).

162. McClellan, *supra* note 24.

163. *Clapper*, 133 S. Ct. at 1151; McClellan, *supra* note 24.

In a case actually involving a data breach, *Krottner*, the Ninth Circuit held "[t]he mere danger of future harm, unaccompanied by present damage, will not support a negligence action."[164] Thus, the plaintiffs' claims regarding spending time monitoring their credit, checking their bank accounts, and placing fraud alerts on other credit cards—all stemming from a danger of future harm but creating no present monetary cost—did not establish an injury for their claim.[165]

Finally, in *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, the United States District Court for the Southern District of California applied the Ninth Circuit's logic in *Krottner* and held that "without specific factual statements that [p]laintiffs' Personal Information has been misused, in the form of an open bank account, or un-reimbursed charges, the mere 'danger of future harm, unaccompanied by present damage, will not support a negligence action.'"[166] There, a class of consumers brought a claim against Sony for failure to safeguard personal and financial information using industry-standard protocols, which created a foreseeable harm to the plaintiffs when the PlayStation Network was breached by a hacker.[167] The court held that actual identity theft of some sort was required in order to establish a cognizable injury.[168]

Overall, as illustrated above, the circuit splits regarding the standing and injury requirements in data-breach cases create inconsistency among jurisdictions. In addition, these cases demonstrate that pursuing a claim can be difficult unless the plaintiff is able to establish a nexus between the data breach and the identity theft, whereby harm from the breach, such as a resulting identity theft, can be clearly shown. When a data breach occurs, but it is uncertain whether the plaintiff's information was taken or no resulting harm is promptly incurred other than mitigation costs to prevent future identity theft, meeting the requirements of standing and injury may be difficult.

D. The Difficulty of Class Action Lawsuits

Another impediment to plaintiffs seeking recovery from corporate data breaches is the difficulty of bringing a class action lawsuit. As most data breaches involve thousands, if not millions, of consumers' personal information, class actions may be an appropriate remedial vehicle.[169] However, even when these suits are successful, the settlements typically are not large enough to compensate victims for their damages.[170] This is a common problem for class action lawsuits

---

164. *Krottner*, 406 F. App'x at 131.

165. Krottner v. Starbucks Corp., 628 F.3d 1139, 1141 (9th Cir. 2010); *Krottner*, 406 F. App'x at 131.

166. 903 F. Supp. 2d at 963 (citing *Krottner*, 406 Fed.App'x at 130).

167. *Id.* at 950.

168. *Id.* at 962–63.

169. *See* Kenneth S. Canfield, *Advantages and Disadvantages of Class Actions From a Plaintiff's Lawyer's Perspective*, 28 THE BRIEF 58, 58–61 (1999) (discussing the requirements for class action certification).

170. *See* NBW, *The Convergence of Data, Identity, and Regulatory Risks*, MAKING BUS. A LITTLE LESS RISKY BLOG (June 13, 2011, 7:54 PM), http://lessrisky biz.blogspot.com/2011/06/convergence-of-data-identity-and.html; Marianne Kolbasuk McGee, *Settlement in AvMed Breach Suit*, DATA BREACH TODAY (Oct. 31, 2013), http://

where the stakes for individual class members are too low to warrant individual suits.[171] And, most class action suits rarely even achieve a settlement because they are often dismissed for not meeting standing and injury requirements.[172]

For example, in 2006, ChoicePoint, a data broker, agreed to a $10 million settlement when consumer–victims brought a class action suit after 163,000 records containing personal information such as social security numbers, bank information, and credit card information were stolen, resulting in at least 800 cases of identity theft.[173] This settlement, while considered to be "huge," in reality only comes out to approximately $61.35 per record.[174] When compared with the estimated cost of a data breach (approximately $157 per record),[175] these settlements clearly do not compensate victims for the cost of a breach.

A more recent data-breach class action lawsuit against AvMed, settled in 2013 for $3 million.[176] There, 1.2 million peoples' information was stolen, but only 460,000 people were entitled to receive $10 for every year they paid insurance premiums to AvMed, with the maximum compensation set at a mere $30.[177]

But what is the average cost of identity theft per consumer? A data breach comes at the cost of approximately $631 and 33 hours spent resolving the issue.[178] Credit monitoring alone, even if identity theft has not occurred, costs on average $120–$180 per year.[179] Clearly, even a "huge" settlement resulting in $61.35 does not come close to covering these costs, especially when the costs of the class action litigation itself must also be deducted from the settlement. And, the costs of a class action lawsuit—including the expense and delay of fighting certification, difficulties with settlement, procedural issues, and overall increased expense—can

---

www.databreachtoday.com/settlement-in-avmed-breach-suit-a-6188; *contra* ZURICH, *supra* note 22, at 5.

171. Christopher R. Leslie, *The Significance of Silence: Collective Action Problems and Class Action Settlements*, 59 FLA. L. REV. 71, 101–02 (2010).

172. ZURICH, *supra* note 22, at 5; *see supra* Part II.B.

173. ZURICH, *supra* note 22, at 5; Jaikumar Vijayan, *ChoicePoint to Pay $10M to Settle Last Breach-related Lawsuit*, COMPUTER WORLD (Jan. 28, 2008), http://www.computerworld.com/s/article/9059659/ChoicePoint_to_pay_10M_to_settle_last_breach_related_lawsuit; Press Release, FTC, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), http://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.

174. ZURICH, *supra* note 22, at 5.

175. *Data Breach Trends & Stats*, *supra* note 3 (citing SYMANTEC, INTERNET SECURITY THREAT REPORT VOLUME 17 (2012); PONEMON INST. & SYMANTEC, *supra* note 4); Hamilton, *supra* note 1.

176. McGee, *supra* note 170.

177. *Id.*

178. Justine Rivero, *Three New Ways to Protect Your Identity in 2012*, FORBES (Jan. 3, 2012 7:07 PM), http://www.forbes.com/sites/moneywisewomen/2012/01/03/three-new-ways-to-protect-your-identity-in-2012/.

179. *Id.*

be large.[180] Thus, even when successful, class actions may not compensate the average consumer for the losses incurred after a data breach, only demonstrating further the need for reforming the current data-breach notification regime in order to provide a better, more adequately compensatory remedy for consumers.

III. ANALYSIS OF POSSIBLE SOLUTIONS

As previously discussed, there are many issues with the current state of data-breach notification law.[181] First of all, 47 states have their own data-breach notification laws, and these laws vary, sometimes significantly.[182] Thus, a company experiencing a data breach where victims are citizens from multiple states may encounter difficulty complying with each states' laws.[183] Second, even when a person has been notified of a data breach pursuant to their state's notification law, their options to hold the company who experienced the breach liable are limited.[184] Most states do not provide a civil cause of action for consumer–victims of data breaches, so already existing means of recovery in civil suits (such as negligence, breach of contract or implied contract, and breach of fiduciary duty) must be adapted to cover data breaches.[185] Most often, these claims are dismissed in federal courts because standing and injury requirements cannot be met. And, even when such claims are successful, the cases—typically brought as class action lawsuits—do not yield nearly enough to adequately compensate each plaintiff.[186]

Because of these issues with the current status of data-breach laws and the increasing prevalence of data breaches,[187] it is clear that changes need to be made in order to render the law more effective in preventing data breaches from occurring and providing consumers with a remedy when breaches do occur. The following Subpart will explore how various proposed changes to the law can effectuate these goals. Due to the realities of our political system, a combination of either a strong national law or a government agency regulating data-breach notification laws, as well as the possible use of the insurance industry to reduce overall risk, would be the most efficient and effective solution.

A. A Proposed National Law

One recent proposed change to data-breach notification laws, with some popularity, has been a push for a national law to preempt the 47 diverging state

---

180. Jonathan D. Glater, *Study Disputes View of Costly Surge in Class-Action Suits*, N.Y. TIMES, Jan. 14, 2004, at C1–C2.

181. *See supra* Part II.

182. Benzing, *supra* note 20.

183. *Id.*

184. *See supra* Part II.B.

185. DATA BREACH CHARTS, *supra* note 42, at 13–14; Ballon, *supra* note 110; ZURICH, *supra* note 22, at 4.

186. *See supra* Part II.D.

187. The latest daily data breaches may be found on SC Magazine's Data Breach Blog at THE DATA BREACH BLOG, *supra* note 1.

laws.[188] In conjunction with this push, on June 20, 2013, Senator Patrick Toomey introduced the Data Security & Breach Notification Act of 2013 ("DSBNA") into the U.S. Senate.[189] The DSBNA would require "entities to take 'reasonable measures' to protect and secure data in electronic form containing 'personal information.'"[190] In addition, like existing state laws, the DSBNA would require entities to notify individuals when unencrypted data is compromised, or when the entity reasonably believes the data has been accessed and acquired in such a manner that might reasonably lead to identity theft or actual financial harm.[191]

One major difference from the existing state law regime is that the FTC would enforce the DSBNA.[192] This means that DSNBA violations would be treated as unfair or deceptive acts or practices under § 5 of the FTC Act,[193] with a maximum civil penalty of $500,000.[194] Also, the DSBNA would require that breaches exceeding 10,000 people be reported to the Secret Service or Federal Bureau of Investigation.[195] However, the DSBNA does not provide consumers with any private cause of action.[196] In addition, it contains no fixed notification timelines—it only requires that notification be made as "expeditiously as practicable and without unreasonable delay."[197] There is also no requirement that state attorneys general be informed, and the proposed bill has no credit bureau reporting provision.[198]

The likelihood of Congress passing any federal data-breach notification law is likely very slim. Thus, the DSBNA will probably not become a reality due to bipartisan disagreement about what security measures should be considered reasonable and how broad the definition of "personal information" should be.[199]

---

188. McMeley, *supra* note 28; Data Security & Breach Notification Act of 2013, S. 1193, 113th Cong. § 6 (2013).

189. Data Security and Breach Notification Act of 2013, S. 1193.

190. McMeley, *supra* note 28.

191. *Id.*

192. *Id.*

193. 15 U.S.C. § 45 (2006).

194. Data Security & Breach Notification Act of 2013, S. 1193, § 4(a)(1), (c)(1)-(3); McMeley, *supra* note 28.

195. Data Security & Breach Notification Act of 2013, S. 1193, § 3(a)(2).

196. *Id.* at § 4(d); McMeley, *supra* note 28.

197. Data Security & Breach Notification Act of 2013, S. 1193, § 3(c)(1).

198. *Id.*

199. GOVTRACK, *supra* note 28 (giving the DSBNA only a 2% chance of being enacted); McMeley, *supra* note 28. The DSBNA defines personal information as:

> [A]n individual's first name or first initial and last name in combination with any 1 or more of the following data elements for that individual:
> (i) Social Security number.
> (ii) Driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity.
> (iii) Financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account.

Data Security & Breach Notification Act of 2013, S. 1193, § 5(5)(A).

This same bipartisan disagreement has led to the death of numerous bills similar to the DSBNA over the past decade.[200]

Even if it were enacted, the DSBNA has several debilitating limitations, rendering it an undesirable change to the current data-breach notification regime. While it will make compliance for companies easier—as they will only have one statute to comply with when a breach occurs rather than a possible 47—it would weaken the injured individuals' remedies and do nothing to help further minimize data-breach occurrences. By not providing a private cause of action, the DSBNA would strip citizens in 14 states of the private cause of action already created by state law. In addition, capping civil penalties at $500,000 may not be a deterrent for some companies. Such a small amount, compared with successful class actions that have settled for millions, may actually shield companies from the higher liability that they currently face. Lastly, the DSBNA's vague definition of what "reasonable measures" companies must take to protect data, and the uncertain time frame for notification, make the DSBNA, at best, a weak method for protecting consumers and preventing data breaches. Therefore, although a national data-breach notification law *could* be effective, the DSNBA would not be.

This Note proposes three solutions that would create a stronger national data-breach notification law. First, the fines for breaches should be increased to an amount that is more likely to incentivize entities to invest in protecting data and minimizing breaches. When the cost of a breach is less than the cost to invest in better data protection, companies will not choose to make the investment. However, by raising the cost of a penalty to a point where it makes investment more cost efficient, companies will have the incentive to make it.[201]

Second, a national law should better define which reasonable measures companies must take in order to protect personal information. A best practice or standard should be set—perhaps through a regulatory agency that could be responsible for keeping such standards up to date[202]—so that entities better understand in what ways they must protect consumers' personal information. A uniform standard would be more efficient in preventing breaches from occurring in the first place and would be more widely instituted. These best practices would also allow for a negligence standard to be adopted for entities that do not comply with them. Additionally, they would also be instructive in resolving the circuit spilt, which has been created by the application of ill-fitted causes of action to claims regarding data breaches. One aspect of these standards could be to mandate personnel training for employees, according to their duties, on data breach prevention and personal information protection. As two-thirds of data breaches are caused by human or system error—including situations where employees do not handle personal information properly, government or industry regulations are

200. McMeley, *supra* note 28.

201. This is a simple cost-benefit analysis, in which the costs of a course of action are compared with the benefits. *See Cost-Benefit Analysis*, MIND TOOLS, http://www.mindtools.com/pages/article/newTED_08.htm (last visited Oct. 27, 2014).

202. *See infra* Part IV.B.

violated, and hardware containing unencrypted information is stolen—mandating employee training could help prevent these breaches.[203]

Third, a national law should provide consumers a remedy through a private cause of action, or a mandate that an entity provide individuals with the option to enroll in a credit monitoring service paid for by the entity for a set number of years following a given data breach.[204] As a private cause of action may be costly for both the company and the consumer, automatically providing an option to enroll in credit monitoring services, which may cost $120–$180 per year,[205] may be the most economically efficient solution for both parties. With either option, however, individuals will still have a remedy, and there will be an incentive for companies to minimize data breaches.

Therefore, although the reality of bipartisan disagreement may prevent the passage of such a national statute at all, as it has for the past decade,[206] a strong national data-breach notification law, if written correctly, could be effective in both preventing data breaches from occurring and providing consumers with a remedy when they do.

B. A Government Regulatory Agency

Given the current ineffectiveness of Congress—the first session of the 113th Congress passed fewer laws than any other Congress since 1947—providing an existing government regulatory agency the authority to administer and enforce data-breach policy may be a more realistic alternative to a stronger national law.[207] Although Congress may need to enact a bill in order to grant a federal agency the power to regulate data breaches, as compared to enacting a more specific statute like the DSBNA, enabling legislation leaves the details of the regulation to the agency to promulgate. Accordingly, this course of action would be more likely to pass through Congress with fewer bipartisan issues.[208]

Like HIPAA, whereby Congress granted regulatory authority to the DHHS,[209] power to regulate data-breach notification law could be given to the

---

203. *Data Breach Trends & Stats*, *supra* note 3 (citing Gartner, *supra* note 16); Hamilton, *supra* note 1.

204. Target voluntarily offered free credit monitoring services to all customers who shopped in their U.S. stores. *Target to Offer Free Credit Monitoring to All Guests*, TARGET (Jan. 10, 2014), https://corporate.target.com/discover/article/Target-to-offer-free-credit-monitoring-to-all-gue.

205. Rivero, *supra* note 178.

206. McMeley, *supra* note 28.

207. Molly Jackman et al., *Congressional Moneyball: Measuring Legislative Effectiveness*, BROOKINGS (Jan. 14, 2014, 11:30 AM), http://www.brookings.edu/blogs/fixgov/posts/2014/01/14-congress-moneyball-gridlock-slegislation-jackman.

208. *See* Sidney A. Shapiro & Robert L. Glicksman, *Congress, The Supreme Court, and the Quiet Revolution in Administrative Law*, 1988 DUKE L.J. 819, 823 (stating that for political and institutional reasons, a broad delegation of authority may prevent disagreements over particular issues, which by themselves would keep Congress from obtaining a consensus).

209. CTR. OF DISEASE CONTROL & PREVENTION, HIPAA PRIVACY RULE AND PUBLIC HEALTH: GUIDANCE FROM CDC AND THE U.S. DEPARTMENT OF HEALTH AND HUMAN

already-existing FTC. The task of regulating data breach law seems to fall most naturally with the FTC, as its goal is to protect consumers and maintain competition in the market.[210] The idea that the FTC would be a natural fit is further supported by the DSNBA's proposal to grant enforcement authority to it.[211]

By granting the FTC authority to regulate and enforce national data-breach law, the law itself would be more likely to keep pace with changing technology as regulatory agencies can update their regulations more easily than Congress can pass new statutes or amend older ones.[212] As previously mentioned, it is estimated that cybercrime overall will continue to grow at a rate of 10% yearly through 2016.[213] Additionally, in recent years mobile devices have become increasingly connected to, and remotely accessible from, the Internet,[214] creating new vulnerabilities that may be exploited in order to gain access to data.[215] Thus, being able to adapt quickly to changing technology could be an important advantage of delegating regulatory authority to a federal agency, as opposed to creating a national statute like the DSNBA.[216]

SERVICES (2003), *available at* http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e 411a 1.htm.

210. *About the FTC*, FTC, http://www.ftc.gov/about-ftc (last visited Sept. 24, 2014).

211. *See* McMeley, *supra* note 28.

212. Cass R. Sunstein, *Law and Administration After* Chevron, 90 COLUM. L. REV. 2071, 2088 (1990) (stating that "Congress is unable to amend every statute to account for . . . changes . . . . Here . . . , administrators are in a far better position . . . to interpret ambiguous statutes in a way that takes account of new conditions."). For further information on how regulations are enacted and amended, see OFFICE OF THE FED. REGISTER, A GUIDE TO THE RULEMAKING PROCESS (2011), https://www.federalregister.gov/uploads/2011/01/the_ rulemaking_process.pdf.

213. *Data Breach Trends & Stats*, *supra* note 3 (citing PONEMON INST. & SYMANTEC, *supra* note 4).

214. Dawn Simmons, *The Dark Side of Technology – the evolution of cybercrime*, XL GROUP, *available at* http://xlgroup.com/~/media/f901ba2df00541a6a18400f6 e93f1ccc.pdf.

215. *Id.*

216. There are also many arguments against government regulation that have been proffered. For example, it has been argued that government regulation is "an impediment to corporate and small business profits, and a waste of precious time and effort . . . ." Marc Davis, *Government Regulations: Do They Help Businesses?*, INVESTOPEDIA, http://www.investopedia.com/articles/economics/11/government-regulations.asp (last visited Oct. 27, 2014). Additionally, government regulation has been called "cumbersome, confusing, expensive, inefficient, vaguely 'unconstitutional,' and, ultimately, counter-productive, because [it hurts] the very businesses and industries [it was] established to protect." David Macaray, *We Need More Government Regulation of Businesses . . . Not Less*, HUFFINGTON POST (June 19, 2013, 12:49 PM), http://www.huffingtonpost.com/david-macaray/we-need-more-government-r_b_3456640.html. However, government regulation may be especially needed in cases of "market failure," wherein the free market either fails to achieve maximum efficiency or does not respond to important needs, such as health care or workplace safety provisions. Tibor R. Machan, *Government Regulation of Business: The Moral Arguments*, THE FREEMAN (July 1, 1988), http://fee.org/the_freeman/detail/ government-regulation-of-business-the-moral-arguments. Thus, in these situations, government regulation can also serve to protect consumers and to "provid[e] financial,

One way in which a federal agency could be guided in regulating national data-breach notification policy could be through the "Final Framework" produced in President Obama's Executive Order Improving Critical Infrastructure Cybersecurity.[217] Released on February 13, 2014, the Framework provides "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[218] Some specific recommendations include updated virus protection, multiple-factor authentication, methods to ensure confidentiality of data, maintaining current security software patches, employee training, and the adoption of cybersecurity requirements across market segments.[219] This Framework could be used to develop a set of best practices—defining what "reasonable measures" companies should be taking to protect consumers' personal information.

Therefore, enabling legislation granting a federal administrative agency, like the FTC, the power to regulate and enforce national data-breach notification law could solve the politically charged problems that come along with enacting a national statute like the DSBNA. Enabling legislation would allow the FTC to provide regulations that more effectively prevent data breaches from occurring and provide consumers with a remedy when they do.

C. The Use of The Insurance Industry

In conjunction with adopting a stronger national data-breach notification law or granting regulatory authority to a federal agency, the insurance industry could also assist in achieving the goal of minimizing data-breach occurrences, which would benefit both commercial entities and consumers. This is because insurance companies could create incentives for entities to become better at protecting personal information by requiring that the insured minimize risk in order to obtain a policy and in order to lower its rates.

Currently, commercial general liability and errors and omissions policies do not commonly cover claims for data breaches.[220] Therefore, in order to obtain coverage, companies need to purchase specialized policies.[221] The combination of both a rise in data-breach occurrences and the possible implementation of a stronger national law providing a remedy for consumer–victims—either through a civil cause of action or mandatory credit monitoring—could increase the demand for these specialized policies in order to limit an entity's liability. Thus, this demand would lead insurance companies to develop standards that insureds would have to follow in order to minimize risk and lower their policy premiums, further

---

advisory and other forms of service to the business community." Davis, *supra*. The security of data containing personal information may be considered one of these market failures, in which companies are not responding to the important needs of consumers.

217. Exec. Order No. 13636, 78 C.F.R. 11739 (2013).

218. *Id.*; Brian S. Gocial, *Improving Cybersecurity—The Road Ahead*, LEXOLOGY (Mar. 3, 2014), http://www.lexology.com/library/detail.aspx?g=72c26b9d-16eb-4cb4-9ed1-4222446b0ba2.

219. Gocial, *supra* note 218.

220. ZURICH, *supra* note 22, at 8.

221. *Id.* at 8–9.

incentivizing data-breach prevention.[222] Additionally, the development of these standards would benefit both consumers and companies by decreasing data-breach occurrences overall.

On the other hand, insurance may be less effective in providing consumers with a remedy *after* a data breach has occurred. For example, consumers can purchase identity theft insurance policies for anywhere from $20–$100 a year.[223] However, these policies "'[do] not cover direct monetary losses incurred as a result of identity theft.'"[224] Instead, the policies cover the expenses of dealing with identity theft such as "the costs of making phone calls and copies, mailing documents and possibly legal bills."[225] Additionally, the deductibles can range anywhere from $100–$1,000, where the average cost to a consumer to correct identity theft is only $1,500.[226] Thus, these insurance policies may not be worth the cost to the average consumer.

Along similar lines, credit monitoring may also not be worth the cost unless an individual has a reason to fear their identity may be stolen.[227] While credit monitoring services can spot things that are reported to a credit-reporting agency, they do not spot every kind of identity theft.[228] However, broader services have begun to be offered by credit monitoring services such as public records, database, and website monitoring.[229] In addition, credit monitoring services are generally $120–$180 per year.[230] Thus, this kind of protection may only make sense if individuals are concerned that they may be victims of identity theft, such as after a known data breach has occurred.[231] Therefore, it may be more economically sound for many consumers to get free annual credit reports and closely monitor personal financial accounts.[232]

Insurance and credit monitoring may be more effective at preventing data breaches from occurring than the current scheme, but are less likely to provide consumers with a remedy when they already have fallen victim to identity theft in the past. Thus, insurance policies alone are not a viable solution to the problems

---

222. Insurance companies' perspectives on risk management in cyber security matters were recognized by President Obama in his Executive Order Improving Critical Infrastructure Cybersecurity. *See* Eric Chabrow, *Identifying Gaps in Cyber Framework: Experts Gather in Dallas to Refine Best Practices Guide*, GOVINFOSECURITY (Sept. 11, 2013), http://www.govinfosecurity.com/identifying-gaps-in-cyber-framework-a-6058.

223. Herb Weisbaum, *Why ID Theft Insurance Might Not Be Worth It*, NBC NEWS (May 8, 2006), http://www.nbcnews.com/id/12692565/ns/business-consumer_news/#.UuL93hDn-M9; Liz Weston, *Is Credit Monitoring a Waste?*, MSN MONEY (Aug. 20, 2012), http://money.msn.com/credit-rating/is-credit-monitoring-a-waste-liz-weston.

224. Weisbaum, *supra* note 223.

225. *Id.*

226. *Id.*

227. Allie Johnson, *Credit Monitoring Services: Pros, Cons and How to Pick One*, FOX BUSINESS (Feb. 24, 2011), http://www.foxbusiness.com/personal-finance/2011/02/23/credit-monitoring-services-pros-cons-pick/.

228. *Id.*

229. *Id.*

230. *Id.*

231. *Id.*

232. *Id.*

with current data-breach notification laws, and should be seen more as a tool to be used in conjunction with a stronger national law or the grant of regulatory to power over the area to a federal agency.

IV. EVALUATING THE OPTIONS: WHAT SHOULD HAPPEN GOING FORWARD

This Note proposes that any changes to the current data-breach notification law should render it more effective in preventing data breaches from occurring and providing consumers with a remedy when breaches do occur. The DSBNA, as it is currently written, is not strong enough to correct the current issues with data-breach notification law. In order to be effective, a national law should increase costs and liability for companies who experience data breaches, thereby incentivizing entities to invest in better protecting data. In addition, increasing the cost and liability for companies requires that a national law better define reasonable measures that companies must take in order to protect personal information and avoid liability. This could lead to the development of best practices or adaptable standards, increasing the security of data for both companies and consumers. Finally, a national law should give consumers either a civil cause of action against entities who have experienced a data breach and do not comply with reasonable measures or mandate that such an entity provide consumer victims with the option to enroll in a credit monitoring service paid for by the entity for a set number of years.

In the alternative, Congress could enable a federal administrative agency, such as the FTC, to regulate data-breach notification laws and standards. An administrative agency may be better able to adapt to changing technology and industry standards than Congress, because it is much easier for an agency to promulgate regulations than it is for Congress to enact a new law. Thus, regulation by an administrative agency may be better able to prevent data breaches than a strong national law alone.

Insurance policies may help supplement a stronger national law or authorized agency by incentivizing entities to minimize their risk of data breaches and by providing a remedy to consumer–victims. President Obama's Executive Order Improving Critical Infrastructure Cybersecurity may provide some additional insight into what industry standards or reasonable measures for data protection should be. The recent revelation of the National Security Agency cracking most encryption codes shows that this is an area where technology is constantly evolving, and even data we think is safe, in reality, may not be.[233] Therefore, whichever changes to the current data-breach notification regime we enact in the future must provide for industry standards that evolve and change to effectively keep personal information safe.

CONCLUSION

Data breaches, now a common occurrence throughout the world, are an ever-present threat to both consumers and companies. In 2014, in the United States

233. *See* Nicole Perlroth et al., *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 6, 2013, at A1.

alone, between January 1 and October 21, 621 data breaches had already been reported, exposing 77,890,487 records containing personal information.[234] Adding fuel to this fire is the current state of data-breach notification law in the United States, which is muddled and confusing. In order to be effective, the law should be as clear and easy to comply with as possible, while also meeting the desired policy objectives. This Note argues that, whichever solution is implemented, data-breach notification laws should have two main goals: to minimize the occurrence of data breaches and to provide consumers with a remedy when data breaches do occur. If these two goals can be met, the effectiveness of data-breach notification law will be significantly improved, not only for consumers who desire that their sensitive, personal data be protected and that they have avenues in which to pursue their grievances, but for companies as well who in good faith desire to comply with the law.

Overall, data-breach notification is a complicated and relatively new area of the law that needs much more research and thought. However, it is also an area that poses serious risk for consumers if the correct balance of liability and cost is not found. Data breaches will only continue to occur daily—placing individuals' personal information in jeopardy—until we find this balance.

234. IDENTITY THEFT RESOURCE CENTER, 2014 DATA BREACH STATS 5 (2014), http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf.