RUTGERS LAW RECORD
The Digital Journal of Rutgers School of Law
lawrecord.com

Volume 44 **2016-2017**

HARMED BY A DATA BREACH: CONSUMERS MAY FIND IT EASIER TO PROVE STANDING UNDER SEVENTH CIRCUIT DECISION

JI WON YOON[1]

I. Introduction

Information is transmitted with increasing frequency in the United States.[2] More than seventy-four percent of the people in the United States are capable of using the internet, allowing many people to share content over the web.[3] However, as more and more information is shared, this widespread sharing is subject to certain risks and vulnerabilities. Technological advancements make the transmission of information easier for normal users while also making the theft of such information much easier as well.[4] Data breaches have become a common occurrence in the United

[1] J.D. Candidate 2017, Rutgers Law School; B.A., Political Science and East Asian Languages and Area Studies, Rutgers University.
[2] Kenneth Cukier, *Data, data everywhere*, THE ECONOMIST (Feb. 25, 2010), http://www.economist.com/node/15557443.
[3] Computer and Internet Use in the United States: 2013, U.S. CENSUS BUREAU 3-4=, https://www.census.gov/history/pdf/acs-internet2013.pdf.
[4] Dan Goodin, *How the NSA can break trillions of encrypted Web and VPN connections*, ARSTECHICA (Oct. 15, 2015), http://arstechnica.com/security/2015/10/how-the-nsa-can-break-trillions-of-encrypted-web-and-vpn-connections.

States, with an average of 100 successful cyber-attacks occurring each week.[5] More and more companies have been affected by data breaches and the people whose data that were supposedly safeguarded by these companies have been consequently affected. Major companies including Target and Sony were subject to such breaches, making them spend millions of dollars in harm prevention.[6] These incidents of data breach gave rise to multiple class action suits against major corporations.[7] Although consumers sued the companies claiming damages and negligence, these claims were dismissed by the court due to the lack of standing.[8] Article III, Section 2 of the Constitution limits federal jurisdiction to lawsuits that present an actual case or controversy. Furthermore, in *Clapper v. Amnesty International*, the Supreme Court held that plaintiffs had to prove they are at imminent risk of suffering from a concrete injury.[9] Other circuits, like the Third, followed the holding and dismissed cases that were unable to prove imminent risk.[10] The Seventh Circuit, however, held that class action plaintiffs have standing when they are able to prove an objectively reasonable likelihood that such harm will occur.[11]

This note explores the current affairs of data breaches in the United States and the available remedies for those affected. Part II of this note will discuss the background of data breaches and the specific laws created by the states to protect the people. Part III will discuss the dichotomy between state and federal laws in protecting consumers harmed by such cyber-attacks. Part IV will discuss the

---

[5] Riley Walters, *Cyber Attacks on U.S. Companies Since November 2014*, THE HERITAGE FOUNDATION (Nov. 18, 2015), http://www.heritage.org/research/reports/2015/11/cyber-attacks-on-us-companies-since-november-2014.
[6] Keith Collins, *A Quick Guide to the Worst Corporate Hack Attacks*, BLOOMBERG (Mar. 18, 2015), http://www.bloomberg.com/graphics/2014-data-breaches/.
[7] *Id.*
[8] *Id.*
[9] Clapper v. Amnesty Int'l, 133 S.Ct. 1138, 1147 (2013).
[10] Reilly v. Ceridian Corp., 664 F.3d 38. 41-42 (3d Cir. 2011).
[11] Remijas v. Neiman Marcus, 794 F.3d 688, 693 (7th Cir. 2015).

relevant cases that shaped the remedies available for those people harmed by a data breach and what standards might change with the new Seventh Circuit decision in *Remijas v. Neiman Marcus*.[12] Part V will conclude that consumers being allowed to prove their "substantial risk" of future harm will allow for better protection of consumers harmed by data breaches.[13]

II. Background Information

Data breaches have occurred for many years as unscrupulous people steal private information for their benefit. Previously large scale data breaches were uncommon, but with technological advancements making the sharing of information simpler, planning cyber-attacks has become easier for hackers.[14] Companies are meant to safeguard information and many do with varying degrees of success. There are those, however, that are subject to a data breach due to poor protection standards set in place.[15] There are also instances of breaches that can range anywhere from a simple mistake to outright negligence when standards are not followed by the employees of the companies.[16]

Data breaches are a problem for all parties involved. The companies that experience the breach must respond to the danger and quickly resolve the problem, often undergoing extraordinary costs to prevent further damages.[17] When dealing with sensitive information, companies these days must protect the information by multiple means. If the companies fail to do so they could be liable

---

[12] *Id.*
[13] *Id* at 693.
[14] Kevin Granville, *9 Recent Cyberattacks Against Big Businesses,* N.Y. TIMES (Feb. 5, 2015), http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html.
[15] Stephen Dinan, *Congress ponders: OPM data breach could total 32 million Americans*, WASH. TIMES (June 24, 2015), http://www.washingtontimes.com/news/2015/jun/24/congress-ponders-opm-data-breach-could-total-32-mi/?page=all.
[16] Dave Lewis, *US Healthworks Suffers Data Breach Via Unencrypted Laptop*, FORBES (June 1, 2015), http://www.forbes.com/sites/davelewis/2015/06/01/us-healthworks-suffers-data-breach-via-unencrypted-laptop.
[17] Bill Hardekopf, *An "Average" Cyber Crime Costs a U.S. Company $15.4 Million*, FORBES (Oct. 17, 2015), http://www.forbes.com/sites/moneybuilder/2015/10/17/an-average-cyber-crime-costs-a-u-s-company-15-4-million.

for damages by either state or private action.[18] Individual consumers whose information was breached also face problems as their information could result in identity theft.[19] Once a company is subjected to a data breach, there is much distrust towards it; the consumers believe that the company should have done more to protect their information. Although such breaches would have happened even if strict security standards were applied, it does not stop consumers from finding the company at fault.[20] This is extremely apparent with the multiple data breaches that recently occurred. [21] The company could have adequate security measures in place to protect sensitive information, but consumers will still fault the company for failing to take greater action.[22]

Most data breaches fall under four categories. The four general categories are: hacking, physical theft or loss, inadvertent exposure, and misuse of information.[23] The following paragraphs will discuss the categories and analyze which categories could potentially cause the greatest loss of faith for companies affected by data breaches.

Data breaches as a result of hacking is the largest category.[24] Most high-profile cases of data breaches fall under this category as hackers aim to collect large volumes of information from the companies and government agencies they target. Data breaches as a result of hacking are frequently in the news, such as the OPM breach which caused the information breach of twenty-one million former and current U.S government employees and the Anthem health insurance hack which

---

[18] OFF. OF THE N. Y. ATT'Y GEN., INFORMATION EXPOSED: HISTORICAL EXAMINATION OF DATA BREACHES IN NEW YORK STATE, http://www.ag.ny.gov/pdfs/data_breach_report071414.pdf (last visited April 17, 2017).
[19] Hadley Malcolm, *Target Sees Drop in Customer Visits After Breach*, USA TODAY (Mar. 11, 2014), http://www.usatoday.com/story/money/business/2014/03/11/target-customer-traffic/6262059.
[20] Hardekopf, *supra* note 14, at 6.
[21] OFF. OF THE N. Y. ATT'Y GEN., *supra* note 15; Companies that become affected by data breaches see a drop in customers after the incident becomes public.
[22] *Id.*
[23] Hardekopf, *supra* note 14, at 7.
[24] Julie Hirschfield Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html.

allowed hackers to obtain as many as eighty million records of former and current customers.[25] Data breaches as a result of hacking occur with increasing frequency as there are many ways hackers can steal such information. Information is normally stored within a company server for access by employees to adequately assist the needs of their consumers. However, these days information is no longer stored in one location. Information is increasingly present on mobile platforms as people frequently need information in remote locations to efficiently work.[26] Although mobile platforms allow for quick communication, their use is not without its risks. People use their phones to log in to unsecured public wireless networks and these networks can be easily penetrated by hackers.[27]

Physical theft or loss of information can result when company employees are not careful with the information they have. Laptops and phones store personal information but lax workers occasionally leave their devices in random areas with no thought as to what might happen to the devices.[28] The equipment is of value to those wishing to make a quick buck and when such equipment is stolen, the personal information is still stored inside the device.[29] Here, the main objective was to steal the device, but because the personal information is now in the hands of an unauthorized person, the information could be wrongly used, especially if the information is unencrypted.[30] Physical theft or loss is not limited to the stealing of devices that hold such private information. Paper documents that hold personal information can become inadvertently thrown out

---

[25] Dinan, *supra* note 12.
[26] Lewis, *supra* note 13.
[27] *Id.*
[28] John Files, *V.A. Laptop Is Recovered, Its Data Intact,* N.Y. TIMES (June 30, 2006), http://www.nytimes.com/2006/06/30/washington/30vets.html.
[29] *Id.*
[30] Granville, *supra* note 11.

or mislaid when a company moves office or places the documents aside for storage.[31] Mistakes like these can cause harm to consumers.

Inadvertent exposures resulting in data breaches can occur when a company is not careful with its treatment of personal information. Any action by company employees that was intentionally or unintentionally done can fall within this category.[32] For example, documents that are supposed to be disposed of are normally shredded before. But if the information was not shredded or wiped, then it could become available for others to use even though the information was disposed.[33] Accidentally sending emails or mistakenly uploading documents online also falls under this category as unauthorized people now have the opportunity to access such personal information.[34] Inadvertent exposure of information can occur in an instant, whether it be by an employee who posts information on Facebook or by an employee who leaves sensitive information unprotected.[35] All companies must take care to protect information from such inadvertent exposure by taking appropriate steps to maintain security.[36] Keeping private emails separate from personal emails and avoiding disclosure of information on social networking websites can prevent unintentional releases of sensitive information.[37]

---

[31] Harold Brubaker, *Old Fashioned Data Breach: Independence Blue Cross Paper Records Tossed in Trash*, PHILLY.COM (Dec. 28, 2014), http://www.philly.com/philly/business/20141227_Old_fashioned_data_breach__Independence_Blue_Cross_paper_records_tossed_in_trash.html.

[32] OFFICE OF THE CAL. ATT'Y GEN., CAL. DATA BREACH REP.(2016), [hereinafter CAL. DATA BREACH REP.] https://oag.ca.gov/breachreport2016.

[33] *Id.*

[34] Karen Price Mueller, *Bamboozled: Breakwater Beach Security Breach Puts Hundreds of Employee Documents Online,* NJ.COM (July 9, 2015), http://www.nj.com/business/index.ssf/2015/07/bamboozled_breakwater_beach_security_breach_puts_h.html.

[35] *Information Security: Inadvertent Data Exposure,* CISCO http://www.cisco.com/c/en/us/about/security-center/inadvertent-data-exposure.html (last visited Mar. 12, 2016).

[36] CAL. DATA BREACH REP., *supra* note 29.

[37] *Id*; Companies could have official policies put in place limiting use of social networking websites to transmit information about company documents. The problem with this is that many companies use social networking websites to provide information about their products. If the company has a public relations department that uses sensitive

Lastly, the misuse of information can cause data breaches when a company employee compromises personal information by making use of unauthorized privileges or resources.[38] Employees can steal the personal information of the company's consumers and later use that information to make purchases, buy products and more.[39] This category is the least common, however, as only ten percent of all data breaches falls under misuse of personal information.[40]

Among the four general categories of data breaches, any category can cause major problems for the companies affected. The category that could potentially cause the greatest problem, however, is the misuse of information.[41] Even with laws and policies in place, the misuse of data continues to grow and perpetrators can be both individuals and companies.[42] The misuse of data combined with incidents of hacking could potentially be the most dangerous as sensitive data could be accessed by those who wish to use the information in illegal ways.[43] Detecting data misuse poses a great challenge for companies as whether the breach is caused by a malicious purpose or an accidental disclosure, misuse of information can diminish a company's value and reputation.[44]

The misuse of information is especially troubling these days with the large amount of data collection that occurs by both companies and state entities.[45] A company could collect data on their

---

information, there still might be an incident of hacking as their information might be less protected as more people would need to access such information.

[38] OFF. OF THE N.Y. ATT'Y GEN., *supra* note 15.

[39] Liam Stack, *8 Indicted in Identity Thefts of Patients at Montefiore Medical Center,* N.Y. TIMES (June 19, 2015), https://www.nytimes.com/2015/06/20/nyregion/8-indicted-in-identity-thefts-of-patients-at-montefioremedical-center.html.

[40] CAL. DATA BREACH REP., *supra* note 29.

[41] Matt Zanderigo, *Examples of the Misuse of Data*, OBSERVE IT (Apr. 16, 2015), http://www.observeit.com/blog/importance-data-misuse-prevention-and-detection.

[42] *Id.*

[43] Steve Lohr, *Data Expert Is Cautious About Misuse of Information*, N.Y. TIMES: BUS. DAY | TECH. (Mar. 25, 2003), http://www.nytimes.com/2003/03/25/business/technology-data-expert-is-cautious-about-misuse-of-information.html.

[44] CAL. DATA BREACH REP., *supra* note 29; Some people after they learn of the breach tend to limit spending money on the breached company's goods. This distrust tends to last a fair amount of time and even methods to limit information breach such as giving free credit checks for two years does not help alleviate this problem.

[45] Zanderigo, *supra* note 38.

customer's spending habits or collect information about the places they visit by tracking their phone or car global positioning system.[46] People are allowed the privacy of their own actions and by monitoring such actions, they obtain information the public wants to keep private.[47] The problem could become even worse when entities that are meant to protect the public use such information in an immoral manner.[48] Law enforcement have access to citizen's private information; they have the potential to track, record, and store information for an indefinite amount of time regardless of whether a person is a suspected criminal or not.[49] Legal protections are needed to limit the collection, retention, and sharing of sensitive information.[50] People have a reasonable expectation of privacy and there is a fear that someone they do not know or like has access to their information.[51] Without such protection in place, companies and state entities would be free to use private information in any way they wish and this will cause the public to fear they are at risk of identity theft or constant tracking.[52] To better protect the people, laws must be created to limit misuse of data.

III. The Dichotomy of State and Federal Data Breach Laws

---

[46] CAL. DATA BREACH REP., *supra* note 29.

[47] Somini Sengupta, *Privacy Fears Grow as Cities Increase Surveillance*, N.Y. TIMES: TECHNOLOGY (Oct. 13, 2013), http://www.nytimes.com/2013/10/14/technology/privacy-fears-as-surveillance-grows-in-cities.html.

[48] Zanderigo, *supra* note 38 (police found to have used data collected to keep tabs on formers lovers and other people they wished to keep track of); Matt Sledge, *NYPD License Plate Readers Will Be Able To Track Every Car Entering Manhattan*, THE HUFFINGTON POST (Mar. 13, 2013), http://www.huffingtonpost.com/2013/03/13/nypd-license-plate-readers_n_2869627.html.

[49] Zanderigo, *supra* note 38; Lohr, *supra* note 40.

[50] Sledge, *supra* note 45.

[51] CAL. DATA BREACH REP., *supra* note 29; Continuous processing and compiling of data is worrying to people as they view this large amount of information collection as an attempt to monitor their private lives. Things that people would like to keep secret could become known and accessed by many others.

[52] Zanderigo, *supra* note 38; Constant data mining can cause incidents of stereotyping as foreign names are subject to greater attention than English names. This combined with data retention could keep a citizen with a foreign sounding name on a watch list indefinitely as data collection occurs at a rapid pace, without any concern for checking for other key information in events of wrongdoing.

Due to the problem of data breaches that continues to plague consumers with increasing frequency, there had to be ways to protect the consumers from wrongdoings by not only the hackers and personal information thieves but also the problems caused by the companies. A company could have the greatest security methods in place to protect private information from hackers, but all the effort is meaningless if there is no company regulation for dealing with internal dissemination of information.[53] If the data is easily disclosed by the employees that use it, then all the hard work from keeping the data safe from hackers will be for nothing.[54]

It is given that hackers steal information to gain an advantage. After hackers obtain private information, they can use stolen information to accrue money by selling the sensitive data as blackmail or to other companies as a corporate spy.[55] But sometimes the hackers are not the only parties at fault. Due to lax company polices, personal information can easily be transmitted to unauthorized people by mistake or negligence.[56] To better protect the personal information of American consumers, most companies use encryption to prevent anyone from being able to use the information. Encryptions help to a large degree, but are still not a panacea. Hackers can still bypass encryption in order to obtain personal information.[57] There are also cases where physical documents

---

[53] Lewis, *supra* note 13.
[54] Mark Scott & Natasha Singer, *How Europe Protects Your Online Data Differently Than the U.S.*, N.Y. TIMES: TECH. (Jan. 31, 2016), http://www.nytimes.com/interactive/2016/01/29/technology/data-privacy-policy-us-europe.html?_r=0.
[55] Josh Keller, *How Many Times Has Your Personal Information Been Exposed to Hackers?,* N.Y. TIMES: PERS. TECH. (July 29, 2015), http://www.nytimes.com/interactive/2015/07/29/technology/personaltech/what-parts-of-your-information-have-been-exposed-to-hackers-quiz.html; Nicole Perlroth, *Accused of Spying for China, Until She Wasn't*, N.Y. TIMES: BUS. DAY (May 9, 2015), http://www.nytimes.com/2015/05/10/business/accused-of-spying-for-china-until-she-wasnt.html; Corporate espionage can occur when employees steal data from their employers and sell them back to their home country. This problem is constantly occurring in the U.S. and Europe as foreign workers who come to work under a visa sometimes sell back information to their home country. The country that engages in such corporate espionage do so because as a way to bypass intellectual property secrets they wish to use without any payment of royalties.
[56] Lewis, *supra* note 13.
[57] Steven M. Bellovin, *Why Even Strong Crypto Wouldn't Protect SSNs Exposed in Anthem Breach*, ARS TECHNICA (Feb. 5, 2015), http://arstechnica.com/security/2015/02/why-even-strong-crypto-wouldnt-protect-ssns-exposed-in-anthem-breach.

containing sensitive information are stolen, whether by corporate spies or by accident.[58] Large companies are especially at risk since safeguarding large volumes of data requires continuous monitoring. No matter how careful a company is, hackers can still access the database and obtain access to frequently used information that is impossible to keep encrypted while others are using that information.[59]

Because large companies are bound to become targets of data breaches no matter how careful they are, there needs to be ways to protect the people at risk. Previously, there were only computer crime legislations in effect and these legislations dealt more with crimes committed by companies and by consumers.[60] There were no laws in place that would protect consumers from a data breach and there were only a few laws that considered unauthorized access to information a crime.[61] In 2003, California became the first state to require data breach notification laws.[62] The new laws in California required business and state agencies to notify consumers when their personal information was exposed in a security breach.[63] Notice to a California resident of a data breach is required if unencrypted personal information "was acquired, or reasonably believed to have been acquired, by an unauthorized person." [64] Since then California has updated its laws to try and keep up with the vast changes in technology over the years. Nevertheless, it is still hard to make such

---

[58] *Id.* Although spies could steal physical documents containing private information, there are more cases where sensitive information is instead lost or misplaced. When companies grow, and need more office space, documents are sometimes not taken care of properly and become lost during the relocation. Boxes containing information could just be thrown in the trash but until the documents are found, it is unknown if it is actual theft or accidental loss.

[59] *Id.*

[60] Philip J. Hilts, *Computer Raiders Hit Big Credit File*, WASH. POST (June 22, 1984), https://www.washingtonpost.com/archive/politics/1984/06/22/computer-raiders-hit-big-credit-file/d3581cf9-8301-4a99-bae8-9c1742da7d19.

[61] *Id.*

[62] CAL. DATA BREACH REP., *supra* note 29.

[63] *Id.*

[64] CAL. CIV. CODE § 1798.29(a), 1798.82(a) (1977).

efficient changes to the laws.[65] The advancements in technology occur at lightning-fast pace and the law fails to keep up. Laws cannot keep up with the advancements of technology as legislators spend most of their deliberating on how to change the law and then eventually fail to enact such laws to help protect the people.[66]

Although California was the first to create its data breach notification law, other states quickly followed. States like New Jersey and New York created their own data breach notification laws and continue to update their laws in an effort to protect their own consumers.[67] But progress is slow; some states have barely updated their laws since they were first created.[68] The laws were meant to protect the consumers but because the laws were so narrowly tailored when they were first created, some states' laws have failed to adequately protect consumers.[69] The laws, when first enacted, only took into account the technological advancements that were present at that time.[70] Today, there are multiple ways that technology can monitor private information but most state laws consider only those technologies that were present when the laws were first enacted.[71] Moreover, there are even some states that do not even have data breach notification laws.[72] The states of Alabama, New Mexico, and South Dakota do not have a data breach notification law.[73] Although

---

[65] CAL. DATA BREACH REP., *supra* note 29.

[66] There are many states that introduced or are considering date breach notification bills or resolutions to amend existing security breach laws. However, most bills fail to make it out as legislators sometimes view the proposed bills as being too strict on companies or having not enough protection for consumers. These arguments are apparent even in New Jersey as five bills were proposed over the past two years to amend the aging law but failed to become enacted.

[67] N.J. STAT. § 56:8-161, 163 (2013); N.Y. Gen. Bus. Law § 899-aa (2015); N.Y. State Tech. Law § 208 (2010).

[68] *See Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Feb. 24, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[69] *See id.*

[70] CAL. DATA BREACH REP., *supra* note 29.

[71] Most state data breach notification laws require notice when private information consisting of social security numbers, financial account numbers, and driver's license numbers are accessed by an unauthorized person. But today, there are multiple other forms of private information and the laws fail to incorporate such technological advancements.

[72] *See supra* note 65.

[73] *Id.*

there have been efforts to create such laws, sometimes the efforts failed in committee and other times the bills failed to gain the necessary amount of votes due to lawmakers' view that the laws were either too weak to protect consumers or too strong against businesses.[74] Without such laws to protect the consumers, Alabama, New Mexico, and South Dakota are not required by their own laws to notify people in the event of a data breach.[75] As Alabama, New Mexico, and South Dakota do not have a security breach notification law, the companies that do business within the state have no mandatory obligation to notify consumers in event of a breach. Companies can notify their consumers regardless of whether a law exists, [76] but as companies usually lose reputation after disclosure of a security breach, it is unlikely companies will notify without an actual law governing their actions.

Nevertheless, the changes to the other states' data breach laws can still affect those states that do not have one. Texas' security breach requirement of notification is given to "all individuals" and applies to "all persons who conduct business in the state."[77] For example, if a company conducts business in Texas and has customers in Alabama, the company would be required to notify individuals in Alabama even though there is no Alabama law to require notification. This law seems to affect large companies more rather than small companies as large companies have greater

---

[74] *Id.* South Dakota was close to enacting its first data breach notification law but failed to garner the necessary number of votes. Legislators claimed that requiring notice to consumers within forty-five days and even if there is no risk that the information accessed by an unauthorized person would cause harm seemed to be too harsh on companies. This is in contrast with California's law, as the state requires notice even if there is no risk of harm. Notice is still required as long as any unauthorized person gained access to the private information. These differing standards make it hard to enact laws in states that do not focus on the future.

[75] *Id.*

[76] *Cyber Security*, STATE OF ALABAMA CYBER SECURITY http://www.cybersecurity.alabama.gov/ (last visited June 1, 2017); In Alabama, the state has a cyber-crime division that provides a list of guidelines for state entities that were affected by a security breach. However, this guideline is just for state entities and even the state entities have no mandatory requirement to follow the guidelines.

[77] Texas Bus. & Com. Code, § 521.053 (2007).

resources to protect their sensitive information and should be held at greater liability.[78] As large companies conduct business across states, this change is better able to protect consumers and even those people that have no state laws to protect them.

The issue of notification is a key part in many states' security breach notification laws as it provides when and how a company must provide notification in event of a breach. Most states require that once sensitive information is acquired by an unauthorized person, notice is given directly to the person affected.[79] Notice must be given in one of three ways: by written notice, electronic notice, or telephonic notice.[80] Written notice must be given directly to the affected consumer at the most recent address on file.[81] Electronic notice can be given if the company has a known email address of the consumer.[82] Telephonic notice can be given in some states if direct contact is made with the consumer.[83] A confusing aspect of notices is that companies can sometimes provide notice in substitute methods. Substitute notice methods include providing notice on a company's website or through use of major state wide media.[84] State laws have guidelines allowing companies to provide substitute notice if the cost of providing notice exceeds a set dollar amount or the total of affected people exceeds a certain number.[85] Ways of providing notices are various and

---

[78] Larger companies usually conduct business over multiple states so having laws like the Texas law would require notification to even those people in other states.

[79] *See supra* note 65.

[80] *Id.*

[81] *Id.*

[82] The notice provided has to be consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

[83] In most states, messages are not allowed to be left on the phone and have the recordings count as a notice given to the consumer.

[84] When posting the notice on a company website, the notice must be on the first page in large, clear font so that people can easily spot the notice. Statewide media is defined in state statutes to be media outlets that provide services to more than seventy-five percent of the population within the area.

[85] On the high end, substitute notice can be used when the cost of providing notice exceeds two hundred fifty thousand and the amount of people to be notified exceeds five hundred thousand. (California and New Jersey) On the low side, substitute notice can be used when the cost of providing notice exceeds five thousand and the amount of people to be notified exceeds one thousand.

many companies can just send out blanket letters to cover many instances of security breaches.[86] But these methods of providing notice can be detrimental as continuous notices by both mail and media could cause consumers to view such notices with less importance and be unable to determine when they actually suffered a harm.[87]

While the states that do have data breach notification laws try to cover most instances of wrongful personal information acquisition, there is no federal law that does the same. Without a federal security breach notification law, requiring notice of personal information breaches are limited to specific situations. Under federal law, only healthcare providers and financial institutions are subject to laws that govern how to deal with the private information of individuals.[88] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) published national standards for the privacy and security of electronically protected health information.[89] HIPAA requires any health care provider to ensure the confidentiality and integrity of all electronic health records and provide notice to consumers when sensitive information is accessed by an unauthorized person.[90] Additionally, the Gramm-Leach-Bliley Act, also known as the Financial Modernization Act of 1999, provides rules for how financial institutions must deal with the private information of individuals.[91] Financial institutions must implement security programs to protect private information and must also provide

[86] States like California and New York require notice to the state attorney general and the same notice used to notify the attorney general can be used to notify the consumers. Thus, there is little need to specifically tailor such notices to each individual and companies can just write a generic letter the can be used for other instances of a security breach.
[87] This is important to when class action lawsuits for data breaches are actually started as the courts continually state that direct damages have to be suffered or certainly impeding to have a cause for action.
[88] *See* 29 U.S.C. §1181 et seq; 15 U.S.C. §6801.
[89] 42 U.S.C. §1320 et seq.
[90] *See id.*
[91] 15 U.S.C. § 6801 et seq.

customers written privacy notices that explain their information-sharing practices.[92] Other sectors are not subject to federal law and must follow state law.

There have been attempts to create a federal data notification law and many bills have been introduced in Congress since early 2015.[93] However, this comes with its own set of problems; with the enactment of a federal security breach notification law, the states' laws would become preempted by the weaker federal law that would offer less protection for consumers.[94] The weaker federal law would also eliminate state requirements that an attorney general be given notice of any security breach.[95] The law would also no longer require breached companies to provide free identity theft protection services such as credit monitoring and fraud alerts.[96] Most importantly, however, it would only allow the state attorney general to file a civil lawsuit but prevent individuals from suing over a data breach.[97] By disposing of an individual right of action, people would longer be able to claim direct damages after a security breach.[98] This right is one of the most important as without the right to bring an individual claim, all subsequent class action cases would become moot.[99]

Other senators, like Patrick Leahy and Elizabeth Warren, have proposed a different law.[100] The federal law would allow states with broader standards of notification requirements to keep those

---

[92] *Id.*

[93] *See* Adam Levin, *How This Federal Data Breach Law Could Actually Hurt Consumers*, FORBES (Mar. 27, 2015, 6:25 AM), http://www.forbes.com/sites/adamlevin/2015/03/27/how-this-federal-data-breach-law-could-actually-hurt-consumers .

[94] *See* Data Security and Breach Notification Act, S.177, 114th Cong. (2015) (this is the weaker federal law proposed)

[95] *See id.*

[96] *See id.*

[97] *See id.*

[98] Right now, individuals still need to claim direct damages to file for a class action suit.

[99] If the right to bring an individual claim is disposed then there can be no subsequent class action lawsuits meaning the previous decisions by the court will no longer matter. Even if an individual could claim certainly impeding damages there would be no right to bring a claim.

[100] *See* Consumer Privacy Protection Act, S.1158, 114th Cong. (2015).

standards while the states with weaker standards to follow the federal law.[101] For example, states like California and Connecticut that require notice to consumers even when there is no risk of harm would apply this standard on companies; for states with weaker notice requirement standards like New Jersey, companies that conduct business within the state would then follow the federal law.[102] But with strong opposition from other senators, it is unlikely that there will be a federal data breach notification law passed soon.[103]

One major problem in both the states data breach notification law and the proposed federal data breach notification law is that the requirement for notice depends on a harm standard.[104] There are some states that require notice even if the personal information acquired by an unauthorized person and is unlikely to cause harm. But some states and in one of the proposed federal laws, notice is required only if the wrongfully acquired information is likely to cause harm.[105] Harm is evident if the acquired information is likely to result in a case of fraud or identity theft.[106] This harm principle is at the center of not only the proposed data breach notification laws but the cases where consumers were affected by data breaches. For people to succeed on their claim, they need to prove they were directly harmed. If they cannot prove harm, they cannot prove their claim and for people to prove they have standing to bring such a class action suit, they must prove they will be at harm.

---

[101] *See* Cory Bennett, *State AGs clash with Congress over data breach laws*, The Hill, (July 7, 2015), http://thehill.com/policy/cybersecurity/247118-state-ags-warn-congress-against-preempting-data-breach-laws.
[102] Alex Bradshaw, *Consumer Privacy Protection Act is Data Breach Legislation We Can Support*, CENTER FOR DEMOCRACY AND TECHNOLOGY (Apr. 30, 2015), https://cdt.org/blog/consumer-privacy-protection-act-is-data-breach-legislation-we-can-support/.
[103] *Id.*
[104] *See* Matt Zanderigo, *supra* note 38; David Lazarus, *Federal data-breach bill would replace dozens of stronger state laws*, L.A TIMES (Apr. 21, 2015, 5:00 AM), http://www.latimes.com/business/la-fi-lazarus-20150421-column.html.
[105] *See* Zanderigo, *supra* note 38; Lazarus, *supra* note 101.
[106] *See* N.J. STAT. ANN. § 56:8-161, -163; N.Y. GEN. BUS. § 899-aa; N.Y. STATE TECH. § 208.

IV. The standard for proving standing in a data breach suit.

As data breaches become increasingly common, so have incidents of litigation where consumers file large class action suits due to the compromise of their personal information. People bring these claims to the court because they were affected by the security beach and believe they have suffered damages. However, most federal courts dismissed the cases, ruling that the plaintiffs lacked standing and were unable to establish a concrete injury to seek redress from the courts.[107] The standard for class action data breach suits, which was clarified by the Supreme Court's decision in *Clapper v. Amnesty International*,[108] states that the "threatened injury must be 'certainly impeding.'" [109] *Clapper* was a constitutional challenge to the Foreign Intelligence Surveillance Act of 2008, which gave authority to the National Security Agency to engage in eavesdropping to gather information from "persons reasonably believed to be located outside the United States to acquire foreign intelligence information." Nevertheless, this eavesdropping was not allowed on citizens residing within in the U.S. or citizens "reasonably believed to be located abroad."[110] Respondents were attorneys and human rights workers whose work required them to engage in the deepest form of secrecy to protect classified information.[111] Because respondents engage in contact with those the government has a special interest in, respondents believed that the monitoring of these people was very likely to happen under the expanded law.[112] FISA surveillance would target their contacts and

---

[107] Alison Frankel, *The 7th Circuit just made it a lot easier to sue over data breaches*, REUTERS (Jul. 21, 2015), http://blogs.reuters.com/alison-frankel/2015/07/21/the-7th-circuit-just-made-it-a-lot-easier-to-sue-over-data-breaches; other cases where courts dismissed claims due to lack of standing include *Storm v. Paytime, Inc.*, 90 F.Supp.3d 359, 364-69 (M.D. Pa. 2015); *Peters v. St. Joseph Servs. Corp.*, 74 F.Supp.3d 847 (S.D. Tex.2015); *In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litig.*, 45 F.Supp.3d 14, 20-24, 29 (D.D.C. 2014); *Polanco v. Omnicell, Inc.*, 988 F.Supp.2d 451, 469-71 (D.N.J. 2013).

[108] Clapper v. Amnesty Int'l, 133 S.Ct. 1138, 1147 (2013).

[109] *Id.* at 1143.

[110] *Id.* at 1144.

[111] *Id.* at 1145.

[112] *Id.* at 1144.

record some of their conversations and electronic exchanges, communications that respondents wish to keep secret.[113] Due to this eavesdropping, the respondents claimed that their ability to communicate with certain individuals would be compromised and that they would will have to undertake significant changes to their methods of communication at a considerable expense.[114] They argued that they faced a risk of future injury because there was an "objectively reasonable likelihood" their communications with sensitive individuals would be acquired under Section 1881a at some point in the future.[115]

While the district court below held that respondents lacked standing, the Second Circuit reversed, holding that respondents have standing due to the "objectively reasonable likelihood that their communications will be intercepted sometime in the future … [and] they are suffering 'present injuries …stemming from a reasonable fear of future harmful government conduct.'" [116]

Justice Alito, writing for the majority, reversed the respondents' claim of standing, holding that the respondent's claim of future surveillance was based on too much speculation to prove that injury was certainly impeding and thus concluded that the respondents lack standing.[117] The dissent contended that "the occurrence of similar future events is sufficiently certain to support standing" and the standard of "certainly impeding" was never used to deny a right to sue in court.[118] Courts have often found the standard of "probabilistic injuries sufficient to prove standing" and thus the respondents' claims should have been allowed.[119]

---

[113] *Id.* at 1145.
[114] *Id.* at 1145-46.
[115] *Id.*
[116] *Id.* at 1146.
[117] *Id.* at 1151.
[118] *Id.* at 1155.
[119] *Id.* at 1162 (citing *Duke Power Co. v. Carolina Environmental Study Group, Inc.*, 438 U.S. 59 (1978) (finding standing in part due to "our generalized concern about exposure to radiation and the apprehension flowing from the uncertainty about

With the standard set in *Clapper*, cases have been subsequently dismissed for lack of concrete substantial harm. Attorneys could try and get around the standard by filing on behalf of a plaintiff who suffered a concrete injury, meaning that the case would not be dismissed as the main plaintiff could attempt to prove there was a concrete injury.[120] Still, most cases have been dismissed due to the inability to prove the "certainly impeding" requirement.

The dismissal of cases for lack of standing held true in the Third Circuit even before the *Clapper* decision. In *Reilly v. Ceridan Corp.*, appellants claim was dismissed for lack of standing.[121] Respondent Ceridan suffered a breach but it was unknown as to "whether the hacker read, copied, or understood the data."[122] As the appellants did not allege actual misuse of their personal information and only claimed that their information could become misused, the court held that the appellant's claim was based on a speculative chain of events.[123] The allegations of injures were based on a future chain of events that the hacker who gained access to the company's database read the personal information and intended to commit future crimes using that information.[124] The court held that "allegations of hypothetical, future injury do not establish standing" and appellants case was dismissed.[125]

---

the health and genetic consequences of even small emissions."). *See also* Mountain States Legal Foundation v. Glickman, 92 F.3d 1228, 1234-35 (D.D.C. 1996) (plaintiffs attack Government decision to limit timber harvesting; standing based upon increased risk of wildfires); Natural Resources Defense Council v. EPA, 464 F.3d 1, 7 (D.D.C. 2006) (plaintiffs attack Government decision deregulating methyl bromide; standing based upon increased lifetime risk of developing skin cancer).

[120] Lewis, *supra* note 13.

[121] *Reilly*, 664 F.3d at 40.

[122] *Id.*

[123] *Id.* at 42.

[124] *Id.* at 43.

[125] *Id.* at 41; *See also City of Los Angeles v. Lyons*, 461 U.S. 95 (1983) (holding that a plaintiff lacked standing to enjoin the Los Angeles Police Department from using a controversial chokehold technique on arrestees. Although the plaintiff had already once been subjected to this maneuver, the future harm he sought to enjoin depended on the police again arresting and choking him).

Even recently, the court in *In re Horizon*, dismissed the case for lack of standing as a thief stealing two laptops did not prove their personal information was actually accessed and misused.[126] Like in *Reilly* and *Ceridan*, the court held the only importance is if plaintiffs actually suffered an "actual or imminently threatened injury" and not if they incurred risk of future injuries and had to incur costs to protect themselves from future harm.[127]

In order for plaintiff's case to be heard, they had to prove that a concrete injury was imminent or impeding and without that proof, their cases were dismissed.[128] Prior to the *Clapper* decision, courts in the Seventh and Ninth Circuit held that the injury-in-fact requirement is satisfied if plaintiffs allege a credible threat of real and immediate harm despite relying on allegations of future harm.[129] After the Supreme Court decision, however, district courts in the Ninth Circuit generally have not treated *Clapper* as overruling established standing principles and plaintiffs can allege "a credible threat of impending harm based on the disclosure of their Personal Information following the intrusion."[130] On the other hand, most district courts in the Seventh Circuit applied the *Clapper* standard to assess standing in data breach cases and in most cases dismissed cases for

---

[126] *In re Horizon Healthcare Servs., Inc. Data Breach Litig.*, 2015 WL 1472483, at *2 (D.N.J. 2015).
[127] *Id.* at *4.
[128] *See In re Sci. Applications Int'l Corp.*, 2014 WL 1858458, at *8 (". . .since Clapper was handed down last year, courts have been even more emphatic in rejecting 'increased risk' as a theory of standing in data-breach cases ... After all, an increased risk or credible threat of impending harm is plainly different from certainly impending harm, and certainly impending harm is what the Constitution and Clapper require.").
[129] *See Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010); *Pisciotta v. Old National Bancorp.*, 499 F.3d 629, 634 (7th Cir. 2007).
[130] *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014). *See also In re Adobe Sys. Privacy Litig.*, 66 F.Supp.3d 1197, 1211 (N.D. Cal. 2014) (plaintiff must allege "(1) injury-in-fact that is concrete and particularized, as well as actual or imminent; (2) that the injury is fairly traceable to the challenged action of the defendant; and (3) that the injury is redressable by a favorable ruling.").

lack of standing.[131] But with the decision made by the Seventh Circuit in *Remijas v. Neiman Marcus*, the courts applied a similar, but slightly different standard.

The court in *Remijas v. Neiman Marcus*, held that plaintiffs could prove they had standing by showing that they faced a "substantial risk" of future harm.[132] *Remijas* was a case that resulted from the December 2013 data breach of Neiman Marcus when its data systems were infected with malware.[133] The credit card numbers of Neiman Marcus customers were compromised but the company maintained that other personal information was not compromised.[134] Plaintiffs filed a class action suit where some claimed actual fraudulent charges and imminent harm.[135] The district court dismissed the claim for failure to prove standing but the Seventh Circuit court of appeals reversed and remanded, holding that plaintiffs were able to prove standing based on their "substantial risk."[136]

The court determined that *Clapper* does not "foreclose any use whatsoever of future injuries to support Article III standing."[137] Although "highly speculative" chain of events does not establish standing, real and "objectively reasonable" threats are sufficient enough to prove the likelihood of substantial harm.[138] The plaintiffs here knew what information was stolen and knew why the company database was hacked, thus giving rise to an "objectively reasonable likelihood" that harm will occur.[139]

---

[131] *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 688-89 (N.D. Ill. 2014); Strautins v. Trustwave Holdings, Inc., 27 F.Supp.3d 871, 876-79 (N.D. Ill. 2014) (the Remijas decision made on 2014 is the previous decision of the court before the Seventh Circuit Court of Appeals heard the case).
[132] Remijas, 794 F.3d at 693. This is compared to the Clapper standing of proving that the "threatened injury must be 'certainly impeding.'" Clapper, 133 S.Ct. at 1143.
[133] Remijas, 794 F.3d at 690.
[134] Id.
[135] Id at 691.
[136] Id at 692.
[137] Id at 693.
[138] Id.
[139] Id.

Although this case might seem to steer away from *Clapper*, the Seventh Circuit holds that their decision clearly falls under the guidelines of *Clapper*. In *Clapper*, the allegations of future harm were based on speculations but in *Remijas*, there is a chain of events that can occur due to the "objectively reasonable likelihood" of harm.[140] The court cites a footnote in *Clapper* which states,

> cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."[141]

Like many cases, the case in *Remijas* is fact specific and the reason why the court held there was standing is very much dependent on the facts. In *Clapper,* there was no standing because the claim just relies on the fact that the government was eavesdropping on the communication of the U.S. citizens.[142] The respondents claim they were subject to harm but their attempt to prove harm relied on a speculative chain of possibilities and did not show that the future injury they purportedly feared was certainly impending.[143] As the petitioners were unable to prove their claim of future harm, the court held they had no standing. Similarly, in *Reilly* and *In re Horizon*, the case of standing relies on the speculation that personal information was taken and used inappropriately, a fact that was unlikely to be proven.[144] But in *Remijas*, the court knew what information was stolen and through what method the information was stolen. As hackers used malware to specifically steal credit card information, it was not too far removed to believe that credit card information would be fraudulently used.[145] This is compared to *Reilly* and *In re Horizon*; in *Reilly,* it is unknown for what

---

[140] *Id.*
[141] *Id.*
[142] *Clapper,* 133 S.Ct. at 1143.
[143] *Id.* at 43-44.
[144] *Reilly*, 664 F.3d at 40; *In re Horizon*, 2015 WL 1472483, at *2.
[145] *Remijas,* 794 F.3d.

purpose the information was stolen and in *In re Horizon,* it is unknown for what purpose the laptops were stolen.[146] Thus, only when the risk is substantial and proven by the facts do plaintiffs have a cause for standing. In *Remijas,* the harm was demonstrable by the facts and thus, the holding is not a change from *Clapper* but just a reiteration of the requirement to prove the risk of harm.

V. Potential effects on current data breach litigation

Individuals in the Seventh Circuit can now show they face a "substantial risk" of future harm to prove they have standing.[147] The problem now is how to prove such future harm. The Supreme Court in Clapper held that future harm could not be proven based on a speculative future chain of events.[148] "Objectively reasonable" threats, however, are sufficient enough to prove the likelihood of substantial harm.[149] Still the question most courts will face in the future is whether plaintiffs have proved they face a risk of future harm and thus satisfy standing.

Today, more and more incidents are a result of hacking. In 2014, the health care sector had loss and theft of employee devices account for sixty-eight percent of healthcare security breaches. However, the numbers are quite different in 2015 as over ninety percent of security breaches were due to hacking and information technology related incidents.[150] The increase in hacking incidents have to do with the fact that healthcare is moving towards connected care.[151] Connected care is the real-time, electronic communication between a health care provider and patient, including aspects

---

[146] *Reilly*, 664 F.3d at 40; *In re Horizon* 2015 WL 1472483, at *2.
[147] *Remijas*, 794 F.3d at 693.
[148] *Clapper*, 133 S.Ct. at 1143.
[149] *Remijas*, 794 F.3d at 690.
[150] Dan Munro, *Data Breaches In Healthcare Totaled Over 112 Million Records In 2015,* FORBES (Dec. 31, 2015, 9:11 PM), http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#58690be47fd5.
[151] *Id.*

such as remote patient monitoring and email communications between doctors and patients.[152] With more information being transmitted within the healthcare, so is the availability of valuable information for hackers to access.[153] Health care will increase its efforts towards providing better treatment for patients but care little for protecting information security.[154] Money will go towards upgrading healthcare equipment but will go little towards upgrading the antiqued hardware and software that protects such sensitive patient information.[155]

Incidents of hacking could make it easier to prove future harm as people now have their personal information in the hands of unscrupulous individuals. Information obtained as the result of a hacking incident means an individual purposefully decided to steal sensitive information. If information was stolen in this manner, it is not a far stretch to believe that this could cause objectively reasonable threats.[156] Additionally, hackers do not keep the information for themselves; they attempt to disseminate the information to other hackers in hopes they have use for such information.[157] Potentially, a hack on a company's safeguarded information could help prove there are looming threats.

---

[152] Drew Schiller, *The future of connected care: Envisioning the possibilities, overcoming the challenges,* HEALTHCARE IT NEWS (Sept. 2, 2015, 8:52 AM), http://www.healthcareitnews.com/blog/future-connected-care-envisioning-possibilities-overcoming-challenges.

[153] *Clapper,* 133 S.Ct. at 1143.

[154] *Id.*

[155] Breaches likely occur because companies do not upgrade their passwords and encryption standards meaning that hackers find it easy to break into such outdated systems.

[156] Josh Keller, *How Many Times Has Your Personal Information Been Exposed to Hackers?* THE N.Y. TIMES (July 29, 2015), http://www.nytimes.com/interactive/2015/07/29/technology/personaltech/what-parts-of-your-information-have-been-exposed-to-hackers-quiz.html.

[157] Lorenzo Franceschi-Bicchierai, *Hacker Publishes Personal Info of 20,000 FBI Agents*, MOTHERBOARD (Feb. 8, 2016, 3:57 PM), http://motherboard.vice.com/read/hacker-publishes-personal-info-of-20000-fbi-agents (hackers break into a database and start these data dumps solely to obtain large collections of personal information. The hackers then post the information on public forums hoping beneficial information is weeded out from the unnecessary).

Other factual aspects subject to inquiry is whether the company offered any monitoring protection after the security breach. As the court in *Remijas* claimed, Neiman-Marcus offered credit monitoring because there were fraudulent charges that occurred after the breach and it was meant provide service and maintenance to those that received fraudulent charges.[158] The measures employed by the company was in fact evidence of the certainty of harm as the company was trying to monitor future incidents and ensure they did not occur.[159] This is helpful for those plaintiffs trying to prove objectively reasonable future harm for class action suits, but is unhelpful for those actually affected with fraudulent charges.[160] Credit monitoring does nothing to identify or alert individuals when someone has compromised existing payment information.[161] Checking credit reports is helpful to determine no one opened a new credit account but is unhelpful at checking individual fraudulent charges.[162] Mitigation expenses do not qualify as actual injuries where the harm is not imminent.[163] However, if a company offers free credit monitoring services after fraudulent charges actually occurred, it might be a way to prove reasonable harm as the company admits its fault and knowledge of the harm and is attempting to provide relief from the harm.[164] The amount of people affected by fraudulent charges can also be helpful to determine whether there is an objectively reasonable threat of harm. If there are multiple charges affecting a large number of

[158] *Remijas*, 794 F.3d at 692.
[159] *Id.*
[160] Gregory Karp, *Why credit monitoring will not help you after a data breach*, CHICAGO TRIBUNE (Aug. 15, 2014), http://www.chicagotribune.com/business/chi-why-credit-monitoring-will-not-help-you-after-a-data-breach-20140815-story.html.
[161] *Id.*
[162] Credit reports do not show individual charges and do not show debit card charges as well.
[163] *Clapper*, 133 S.Ct. at 1152.
[164] *Remijas*, 794 F.3d at 692.

individuals, it is objectively reasonable that the company database was hacked for the purpose of obtaining personal financial information and using the information for theft.[165]

Moreover, the amount of time that elapsed between the security breach and any purported harm could be a factor in proving injuries. There is no reason to require the plaintiffs "to wait for the threatened harm to materialize in order to sue."[166] "The more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach."[167] Harm can occur right after a security breach or many days afterwards. If the purported harm occurs subsequently after the breach, harm is very easy to prove.[168] However, stolen data may be held for days and even years before being used to commit fraud or theft.[169] Just because the purported fraud could happen many days after does not exclude it from the objectively reasonable possibility that harm could occur. In contrast, if harm does not occur for many years after, it is hard to prove that the harm occurred as a result of the first security breach and not from any other breaches.[170] But as data breach litigation occurs quickly after the breach of information, it is likely that courts will just need to focus on whether it is objectively reasonable that the breach could result in theft later in time.

---

[165] Martha White, *Wendy's Customers Should Start Worrying Right Now,* TIME (Jan. 27, 2016), http://time.com/money/4196058/wendys-hack-fraudulent-charges.

[166] *Remijas*, 794 F.3d at 693 (The court in *Remijas* held that plaintiffs have to prove they are in danger of a substantial risk of harm. They do not need to prove factual harm. This was also the same in *Clapper* where respondents needed to prove certainly impeding harm but nothing in the opinion stated that respondents must prove at present the harm that occurred).

[167] *Id.* (citing *In re Adobe Sys.*, 66 F. Supp. 3d at 1215n.5).

[168] Paul Roberts, *Missing in Michaels Data Breach: Harm To Consumers*, DIGITAL GUARDIAN (Jan. 7, 2016), https://digitalguardian.com/blog/missing-michaels-data-breach-harm-consumers.

[169] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION 29 (2007).

[170] The more time elapsed after a breach the less likely it seems that personal information is still in the hands of thieves. In addition, there is more time for individuals to change numbers and account information, meaning if plaintiffs are unable to prove an objectively plausible risk of harm, they will be unable to claim damages.

V. Conclusion

For there to be less confusion as to whether plaintiffs do have standing to bring their class action data breach claim, there needs to be some guidance by the Supreme Court. With such privacy concerns and the importance of keeping sensitive information safe, the Supreme Court should provider a broader view of standing in some data breach cases, especially those where the company knows the breach is a result of hacking. If the Supreme Court does not address the issue of standing in data breach cases, it seems that courts will continue to distinguish the *Clapper* standard as one that bars claiming damages for future harm. The other option would be to wait for legislation to determine what counts as harm but this seems unlikely. For now, courts aside from the Seventh and Ninth Circuits will distinguish the *Clapper* standard of "certainly impeding" with "substantial risk" and continue to dismiss claims of data breach for lack of standing.[171]

[171] *Clapper*, 133 S.Ct. at 1152; *Remijas*, 794 F.3d at 693.