Western New England Law Review

Volume 41 *41 (2019)*
Issue 2

Article 2

2019

CONSUMER PROTECTION—EXPLORING PRIVATE CAUSES OF ACTION FOR VICTIMS OF DATA BREACHES

Justin H. Dion
Western New England University School of Law, justin.dion@law.wne.edu

Nicholas M. Smith
Western New England University School of Law

WESTERN NEW ENGLAND LAW REVIEW

Volume 41 2019 Issue 2

CONSUMER PROTECTION—EXPLORING PRIVATE CAUSES OF ACTION FOR VICTIMS OF DATA BREACHES

Justin H. Dion[*] & *Nicholas M. Smith*[†]

Data breaches are becoming a norm in modern life. Every year it seems that bigger and bigger attacks are launched, and more and more individuals are harmed. The law has responded by increasing states' ability to prosecute cybercriminals. A glaring hole exists in this protection though. The state is largely an unharmed party. The real harm is done to individual citizens affected by the breaches. Their data is compromised, their identities are stolen, and their livelihoods are placed at risk. This Article will analyze the issue and propose a solution for increased consumer protection in addition to the current criminal punishments.

INTRODUCTION

Consumers increasingly transmit financial and personally identifiable information online to government, banking, and private corporations (collectively "business").[1] Depending on the online transaction, consumers will often electronically transmit their personal demographic information.[2] If engaging in a commercial transaction, the consumer will

* Justin Dion is a Professor of Legal Skills and Director of Bar Admissions Program at Western New England University School of Law.

† Nicholas Smith is a third-year law student and a Note Editor for the *Western New England Law Review*.

1. *See E-Commerce Worldwide—Statistics & Facts*, STATISTA, https://www.statista.com/topics/871/online-shopping/ [https://perma.cc/QX2R-D7WH] ("In 2018, an estimated 1.8 billion people worldwide purchase[d] goods online. During the same year, global e-retail sales amounted to 2.8 trillion U.S. dollars and projections show a growth of up to 4.8 trillion U.S. dollars by 2021.").

2. *See* Boer Deng, *People Identified Through Credit-Card Use Alone*, DICTYNNA'S NET (Feb. 23, 2015, 5:58 PM), http://dictynnasnet.blogspot.com/2015/02/people-identified-through-credit-card.html [https://perma.cc/LD3J-LRLG] (reporting on a study finding that identifying information could be found in credit-card metadata); *see also* Tyler v. Michaels Stores, Inc.,

often transmit personal payment data to the business vendor.[3] This typically includes debit or credit card information consisting of a sixteen-digit account number, card expiration date, and the three-digit card verification value (CVV) number located on the back of the card.[4] It is important to note that the use of credit cards for consumer purchases greatly benefits merchants. In addition to ease of use, studies have shown that consumers are willing to spend significantly more for items when using a credit card as opposed to cash.[5] This information becomes particularly relevant due to the increasing news coverage regarding data theft as it has been extensive over the past several years, particularly after the Equifax data breach was made public in September 2017.[6]

The completion of some commercial online transactions may require that more specific personally identifiable information be transmitted electronically to the business. This includes the consumer's date of birth, all or part of a social security number, annual income, consumer's mother's maiden name, and favorite pet's name.[7]

This online relationship benefits both the consumer and business entity by allowing time efficient and financially expeditious transactions without mailing costs or delays, paper transmittal and storage, and other

984 N.E.2d 737, 743–44 (Mass. 2013) (finding the statutory definition of personal identification information "explicitly nonexhaustive").

3. *See* Miriam Caldwell, *How a Debit Card Works*, THE BALANCE, https://www.thebalance.com/what-is-a-debit-card-2385853 [https://perma.cc/WFP9-CWJN] (last updated May 8, 2019).

4. *See Privacy When You Pay: Credit, Debit, Cash and More*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/consumer-guides/privacy-when-you-pay-credit-debit-cash-and-more [https://perma.cc/AED9-DXNN].

5. *See* Bailey Peterson, *Credit Card Spending Studies (2018 Report): Why You Spend More When You Pay with a Credit Card*, VALUEPENGUIN, https://www.valuepenguin.com/credit-cards/credit-card-spending-studies [https://perma.cc/N639-KUYG].

6. Although reported in September 2017, the breach actually occurred in May 2017, exposing the data of over 143 million people. Many commentators saw this breach as particularly damaging since Equifax is a consumer credit reporting agency that collects and aggregates information of over 800 million individual consumers and more than eighty-eight million businesses worldwide. *See* Lee Mathews, *Equifax Data Breach Impacts 143 Million Americans*, FORBES (Sept. 7, 2017, 10:42 PM), https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#53d7ca59356f [https://perma.cc/AL87-XSW6].

7. *See Online Shopping Tips*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/consumer-guides/online-shopping-tips [https://perma.cc/RY4L-UTBN] (last updated Nov. 7, 2018); *see also How to Avoid Giving Away Your Personal Details Online*, U. BRISTOL, http://www.bristol.ac.uk/infosec/protectyou/how-to-avoid-giving-away-your-personal-details-online/ [https://perma.cc/78ZA-YC7S] (explaining the types of information that many websites use as security questions and how to protect your data online).

human processing efficiencies and costs.[8] Although the increased transmission of online data has allowed businesses to improve efficiency and profitability, the massive amounts of personal and financial data transmitted and stored by businesses have created significant opportunities for data thieves.[9] Those able to illegally acquire and monetize consumer data are then able to commit crimes using this data, without a physical weapon or presence and often across state or national geographical borders. Accordingly, these crimes are very low risk to commit, as local and state law enforcement often lack the technological tools needed to identify the suspects. Further, even if the suspects and their location were identified, lack of resources and jurisdictional restrictions often prevent prosecution.[10] Although the Federal Bureau of Investigation and the United States Secret Service have tools and resources more capable of identifying and prosecuting cyber-criminals, the amount stolen from an individual is often too small to trigger a federal investigation.[11]

Improper data storage and the resulting data theft have exposed enormous amounts of consumer data to unintended third parties, ultimately resulting in billions of dollars in losses.[12] In addition to the recent Equifax breach, significant personal data has also been stolen from Yahoo (three billion accounts were compromised in a 2013 attack),[13] eBay (145 million accounts were compromised in 2014),[14] JP Morgan Chase

8. *See* Katherine Rengel, Comment, *The Americans with Disabilities Act and Internet Accessibility for the Blind*, 25 J. MARSHALL J. COMPUTER & INFO. L. 543, 544 (2008).

9. *See* Brittain Ladd, *Amazon, Target, Walmart and Kroger: The Biggest Problem in E-Commerce Has Finally Been Solved*, FORBES (Sept. 18, 2018, 7:16 AM), https://www.forbes.com/sites/brittainladd/2018/09/18/amazon-target-walmart-and-kroger-the-biggest-problem-in-e-commerce-has-finally-been-solved/#50562e7f9ad7 [https://perma.cc/3MW2-UGA8] ("By 2021, e-commerce sales globally are estimated to reach $4.8 trillion. For a frame of reference, in 2017, Amazon delivered over 5 billion packages just for Prime members. In a word, e-commerce is a *massive* enterprise and it's only getting larger.").

10. *See* Nick Selby, *Local Police Don't Go After Most Cybercriminals. We Need Better Training*, WASH. POST (Apr. 21, 2017), https://www.washingtonpost.com/posteverything/wp/2017/04/21/local-police-dont-go-after-most-cybercriminals-we-need-better-training/?noredirect=on&utm_term=.6ac96f3c91e6.

11. *Id.* ("[C]ybercrime only becomes 'serious' around $200,000 of loss.").

12. *See* Herb Weisbaum, *Data Breaches Cost Consumers Billions of Dollars*, TODAY (June 5, 2013, 12:37 PM), https://www.today.com/money/data-breaches-cost-consumers-billions-dollars-6C10209538 [https://perma.cc/8A3C-4QX5].

13. Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html [https://perma.cc/N95R-P6FX].

14. Andrea Peterson, *eBay Asks 145 Million Users to Change Passwords After Data Breach*, WASH. POST (May 21, 2014), https://www.washingtonpost.com/news/the-

(seventy-six million household accounts and seven million small business accounts were compromised in 2014),[15] and Anthem Blue Cross Blue Shield (up to eighty million records were compromised).[16]

Based on the demand for increased online transactions, from both consumers demanding convenience and business entities pursuing economic efficiencies, the growth of online data transmission is predicted to continue for many years.[17] Accordingly, so too will the occurrences of data theft.[18] Based on the scope of information obtained by businesses in online transactions, it is not surprising that when a data breach occurs, the resulting theft can have devastating and long-lasting consequences for the consumer victim.[19] Unchecked data theft poses a risk to the trust and integrity of the entire online financial system.[20] This Article argues for

switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/?utm_term=.05183e991af5 [https://perma.cc/X25F-KFFJ].

15. Jessica Silver-Greenberg et al., *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES: DEALB%K (Oct. 2, 2014, 12:50 PM), https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/ [https://perma.cc/XLR5-BZHT].

16. Lauren Sporck, *11 of the Largest Data Breaches of All Time (Updated)*, OPSWAT: BLOG (Nov. 22, 2017), https://www.opswat.com/blog/11-largest-data-breaches-all-time-updated [https://perma.cc/N5MZ-ZA7D]. For a comprehensive overview of cybercrime, see Al Pascual et al., *2018 Identity Fraud: Fraud Enters a New Era of Complexity*, JAVELIN (Feb. 6, 2018), https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity [https://perma.cc/EFZ8-9A5L] ("[C]riminals are engaging in complex identity fraud schemes that are leaving record numbers of victims in their wake. . . . In 2017, there were 16.7 million victims of identity fraud, a record high that followed a previous record the year before."). "The amount stolen hit $16.8 billion last year as 30 percent of U.S. consumers were notified [of their] exposure to a data breach last year, an increase of 12 percent from 2016. For the first time, more Social Security numbers were exposed than credit card numbers." *Facts + Statistics: Identity Theft and Cybercrime*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime [https://perma.cc/WVU7-6F82].

17. Fareeha Ali, *U.S. Ecommerce Sales Grow 15.0% in 2018*, DIGITAL COMMERCE 360, https://www.digitalcommerce360.com/article/us-ecommerce-sales/ [https://perma.cc/GU3K-8CHG] (last updated Mar. 13, 2019).

18. *See* Michael Wood, *With an Increase in Online Shopping, Prepare for an Increase in Data Breaches*, FORBES (Feb. 24, 2018, 12:17 PM), https://www.forbes.com/sites/allbusiness/2018/02/24/with-an-increase-in-online-shopping-prepare-for-an-increase-in-data-breaches/#74a98e7ce67b [https://perma.cc/AWG9-7ES9].

19. *See* EQUIFAX, A LASTING IMPACT: THE EMOTIONAL TOLL OF IDENTITY THEFT 1–2 (2015), https://www.equifax.com/assets/PSOL/15-9814_psol_emotionalToll_wp.pdf [https://perma.cc/8AQN-VW6V].

20. Tracy Sharp et al., *Exploring the Psychological and Somatic Impact of Identity Theft*, 49 J. FORENSIC SCI. 131, 131 (2004).

> The majority of [identity theft victims] expressed an increase in maladaptive psychological and somatic symptoms post victimization. Results on the BSI indicated that identity theft victims with unresolved cases, in contrast to those with resolved cases, were more likely to have clinically elevated scores when compared with a normative sample. Relatively similar coping mechanisms were utilized

both expansion of current and creation of new federal and state laws that will empower consumers to have a cause of action and directly hold businesses accountable for damages (including the psychological harm associated with data theft) for improper storage of data and data theft. This would be achieved by: (i) leveraging and expanding existing state consumer protection laws; (ii) more freely utilizing common law remedies (such as fraud, negligent infliction of emotional distress, and breach of contract); (iii) expanding the FTC to include a private cause of action; and (iv) modifying federal laws to better empower consumers (such as EFTA and Regulation-E) or enacting new legislation that requires the holder of consumer personal data to safely store, transmit, and destroy all data in a manner reasonably consistent with industry standards, of which consumers will have a specific cause of action in which they can sue for damages individually or as part of a class action, if a violation thereof occurs. This will incentivize business entities to significantly improve data security, which, in turn, will reduce data theft-related crimes.

This Article will analyze data breaches and identity theft, address existing laws and their flaws, and finally propose a solution. Part I will seek to identify the separate, although related, issues of data breach and identity theft. It will define key terms and seek to explain how data is stolen and how criminals use that data to commit identity theft. Part II will explore current laws and remedies as they relate to privacy and data protection. It will seek to draw parallels between current federal, state, and international laws. Part III will propose a way forward, focusing specifically on what is lacking in current legal solutions and proposing a more appropriate legal remedy drawn from consumer protection laws.

I. DATA BREACH AND IDENTITY THEFT—IDENTIFYING TWO DISTINCT PROBLEMS

This Part of the Article seeks to provide an overview of how data breaches occur and how thieves illegally monetize stolen data. It will explore several important definitions to establish a background for readers on data, breaches, damages, and the internet. It will also explain how hackers use a hidden part of the internet to buy and sell personal information.

---

across victims. The results from this study suggest that victims of identity theft do have increased psychological and physical distress, and for those whose cases remain unresolved, distress is maintained over time.

Id.

A. *Defining Data*

Often confused for one another, "data breach"[21] and "identity theft"[22] are terms that, although interrelated, are distinct.[23] In terms of our discussion regarding data breaches, this Article defines "data" broadly, representing any electronic transmissions which could be used individually or collectively to identify information regarding the status of a person's identity, finances, healthcare, education, or any other information in which there is a reasonable expectation that it will be kept private and not be publicly disclosed or shared with any unrelated third party. In turn, "data breach" means "the loss, theft, or other unauthorized access, other than those incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data."[24] Data breaches can originate from many sources and with varying degrees of malicious intent. Common examples include:

- Co-workers unintentionally including an attachment containing personal data to an email.
- Due to outdated software by a medical billing office, medical records are accessed by a hacker.
- Bank employees send unencrypted emails containing customers' financial data.
- An employee unintentionally opens a file containing malware, which in turn transmits client data to a third-party criminal.
- An attorney opens a file at home using their unsecure personal computer.
- A data host has failed to update their security software, thus permitting data to be stolen by a third party.

---

21. "A data breach is a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so." ADMIN. FOR CHILDREN AND FAMILIES, U.S. DEP'T HEALTH & HUMAN SERVS., LOG NO. ACYF-CB-IM-15-04, INFORMATION MEMORANDUM (2015), https://www.acf.hhs.gov/sites/default/files/cb/im1504.pdf [https://perma.cc/8SRJ-R8VQ].

22. "Identity theft" is defined as "the illegal use of someone else's personal information (such as a Social Security number) especially in order to obtain money or credit." *Identity Theft*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/identity%20theft [https://perma.cc/4U9Q-42DZ].

23. *See* Brandon Ferrick, Comment, *No Harm, No Foul: The Fourth Circuit Struggles with the "Injury-in-Fact" Requirement to Article III Standing in Data Breach Class Actions*, 59 B.C. L. REV. E-SUPPLEMENT 462, 462 (2018) (explaining that, after a data breach, two of the most common harms cited in lawsuits are identity theft and increased risk of identity theft).

24. Veterans' Benefits, 38 U.S.C. § 5727(4) (2019) (defining "data breach").

- A manufacturing executive loses a company laptop containing company trade secrets.

When data is improperly exposed, it is at risk of being taken by an unauthorized third party and also being used to the detriment of the data originator.

B. *Defining Data Breach*

While one may find it troubling to discover that his or her personal data was exposed in a data breach, the exposure may become more serious if the data is then subsequently used in an identity theft crime. Identity theft primarily occurs when cybercriminals obtain information from a data breach and then use it to apply for loans and credit, commit fraud, withdraw money, make unauthorized purchases, or otherwise leverage the information to financially benefit the criminal.[25] Akin to being the victim of a data breach, identity theft can cause significant psychological harm to a victim, as well as financial loss.[26] Although not all data breaches result in identity theft, the fact that compromised information is available to unauthorized third parties can cause significant anxiety and indefinite concern.[27]

Despite enhanced efforts to combat identity theft, the "2017 Identity Fraud Study, released by Javelin Strategy [and] Research, found that $16 billion was stolen from 15.4 million U.S. consumers in 2016, compared with $15.3 billion [stolen from] 13.1 million victims a year earlier. In the past six years, identity thieves have stolen over $107 billion."[28]

---

25. *See Warning Signs of Identity Theft*, FED. TRADE COMM'N (May 2015), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft [https://perma.cc/FFS3-3A93]; Al Pascual et al., *2017 Identity Fraud: Securing the Connected Life*, JAVELIN (Feb. 1, 2017), https://www.javelinstrategy.com/coverage-area/2017-identity-fraud [https://perma.cc/3F8J-NFKY]. In 2016, 6.15% of consumers became victims of identity fraud. Pascual et al., *supra*. Criminals are increasingly moving online, demonstrated by growth in existing card fraud, which saw a significant spike in card-not-present transactions (CNP). *See id.*

26. From the author's experience as a bankruptcy practitioner, it is not uncommon for an individual to file bankruptcy due in part because of debts on their account incurred by someone who has stolen their identity.

27. Ferrick, *supra* note 23, at 480 (explaining that there may not be a legal claim for individuals whose data has been compromised, but whose identities have yet to be stolen, increasing anxiety for these individuals, with no legal remedy).

28. Reuben Jackson, *Finding Ways to Protect Your Online ID Through Blockchain* Innovation, NASDAQ (Mar. 9, 2018, 9:47:28 AM), https://www.nasdaq.com/article/finding-ways-to-protect-your-online-id-through-blockchain-innovation-cm932475; *see* Pascual et al., *supra* note 25; *see also Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, JAVELIN (Feb. 1, 2017), https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-

C. *Defining Data Breach "Damages"*

Another obstacle consumers face in seeking redress is the lack of quantifiable and speculative damages.[29] It is important to note that even if the data is not ultimately used in a manner that results in direct economic harm to the data originator, even the mere knowledge of the breach can cause psychological harm for the victim for years to come due to the anxiety and concern about the use of the data in the future.[30] Following a data breach, the electronic nature of the data means it is available to criminals in perpetuity, and therefore, it is possible that the concern of ongoing psychological harm to the victim may also exist in perpetuity. Courts may require that victims suffer a harm before being able to seek redress, but those same statutes do not define harm.[31] Harm can occur in many forms ranging from easily quantifiable harm, such as specific amounts of money traceable directly to an identity theft, to harms that are difficult to quantify, such as the anxiety and fear of a potential future theft, even if there have been no funds yet stolen.[32] As stated by Daniel J. Solove and Danielle Keats Citron in their article *Risk and Anxiety: A Theory on Data Breach Harms*:

> The law offers a set of tools that can be used to address harm, from compensatory damages to equitable relief (such as injunctions) to remedies (such as unjust enrichment).
>
> Our legal system needs to confront data-breach harms because real costs are borne by individuals and society and because ignoring them results in inefficient deterrence. Courts routinely avoid hard questions and ignore the anxiety people experience and the increased risk that data breaches cause. Yet in other areas of the law, courts have recognized such harms and placed manageable limits on their reach. As we have shown, those legal developments should inform how courts address data-breach harms. A path has been laid to help us work through the complexities of data-breach harms.

---

million-us-victims-2016-16-percent-according-new [https://perma.cc/KZB4-QM8U] (illustrating yearly losses in the table titled "Fraud Losses").

29. *See generally* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013). In *Clapper*, Plaintiffs challenged a provision of the Foreign Intelligence Surveillance Act (FISA) that created new procedures for authorizing government electronic surveillance of non-U.S. persons outside the U.S. for foreign intelligence purposes. *Id.* at 402–04. The Court held that the respondents did not have standing under Article III of the U.S. Constitution because no injury had yet occurred. *Id.* at 422.

30. *See* Ferrick, *supra* note 23, at 475–80 (discussing the circuit split on actual harm of a data breach and the legal strategy of arguing imminent damage).

31. *See id.* at 462–63.

32. *See id.*

> Data-breach harm might often be intangible, but it still is very real. Data harm is frequently risk-oriented, but risk management is a standard part of the way that the modern commercial world operates.[33]

In *Tyler v. Michaels Stores, Inc.*, the Massachusetts Supreme Judicial Court held that under chapter 93, section 105 of the Massachusetts General Laws,[34] a plaintiff can pursue a cause of action even if no actual identity fraud occurred.[35] In *Tyler*, the consumer made purchases at Michaels, a crafts supply store, using a credit card.[36] During the credit card transaction, an employee asked Tyler for her zip code. Tyler, assuming the transmittal of her zip code was required to complete the transaction, gave the employee her zip code.[37] The data sought was not required by the credit card holder, but rather was requested as part of an internal policy of Michaels in which it recorded information about customers who engaged in credit transactions, including their names, zip codes, and credit card numbers.[38] Accordingly, Michaels was able to access Tyler's address and phone number after she gave the cashier her name and zip code.[39] Michaels's then also sent unsolicited marketing materials.[40] The trial court ultimately found Tyler's complaint against Michaels failed as there was no cognizable injury for collecting zip code information under chapter 93A of the Massachusetts General Laws.[41] The court went on to hold:

---

33. *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 785 (2018).

34. MASS. GEN. LAWS ch. 93, § 105(b) (2018) prohibits a vendor from requiring a credit card holder to include additional identifying data on their credit transaction form as follows:

> No person, firm, partnership, corporation or other business entity accepting a check in any business or commercial transaction as payment in full or in part for goods or services shall do any of the following:
> (1) Require, as a condition of acceptance of such check, that the person presenting such check provide a credit card number, or any personal identification information other than a name, address, motor vehicle operator license number or state identification card number of such person and telephone number, all of which may be recorded
> . . . .
> (4) Require, as a condition of acceptance of the check, that a person's credit card number be recorded in connection with any part of a transaction.

Id.

35. Tyler v. Michaels Stores, Inc., 984 N.E.2d 737, 747 (Mass. 2013).
36. *Id.* at 739.
37. *Id.*
38. *Id.*
39. *Id.*
40. *Id.*
41. *Id.*

> Returning to [section] 105(a), there appear to be at least two types of injury or harm that might in theory be caused by a merchant's violation of the statute: the actual receipt by a consumer of unwanted marketing materials as a result of the merchant's unlawful collection of the consumer's personal identification information; and the merchant's sale of a customer's personal identification information or the data obtained from that information to a third party. When a merchant acquires personal identification information in violation of [section] 105(a) and uses the information for its own business purposes, whether by sending the customer unwanted marketing materials or by selling the information for a profit, the merchant has caused the consumer an injury that is distinct from the statutory violation itself and cognizable under [chapter 93A, section 9].[42]

In *Katz v. Pershing, LLC*, the Massachusetts Court again contended with the difficulty of determining whether adequate damages exist. In *Katz*, a Massachusetts brokerage firm used software that permitted its clients' personal information to be disclosed to unauthorized third parties in violation of Massachusetts law.[43] The court ultimately granted the defendant's motion to dismiss for lack of subject matter jurisdiction, ruling that the plaintiff did "not allege that any of her [personal information] ha[d] been lost, stolen, disclosed, or accessed by an unauthorized person."[44] The court agreed with the defendant that "any potential injury that [the plaintiff] might suffer at some point in the future because of a misappropriation of her [personal information] is far too speculative to satisfy standing requirements; therefore, [the plaintiff] has failed to satisfy the injury-in-fact requirement."[45]

Even if victims are able to demonstrate injury-in-fact, they also face challenges based on standing, as state statutes only empower the State Attorney General to file suit.[46] For example, the plaintiffs in *Katz v. Pershing, LLC* brought their suit personally (i.e., it was not a government entity that brought the suit), and they did not seek redress under any data protection statute but merely brought their claim as a breach of contract.[47] In addition, as the *Katz* plaintiffs did not allege any actual harm suffered from the misuse of their data, the court might have been more willing to allow their common law claim to proceed had a quantifiable harm

42. *Id.* at 746 (footnotes omitted).

43. *See* Katz v. Pershing, LLC, No. 10-12227-RGS, 2011 WL 1113198, at *1 (D. Mass. Mar. 28, 2011).

44. *Id.*

45. *Id.*

46. *See* Mass. Gen. Laws ch. 93A, § 4 (2018) (giving the Attorney General authority to bring action in Superior Court for violations of this law).

47. *Id.*

occurred. Based on this case, in conjunction with other state case law, Massachusetts courts are reluctant to allow lawsuits if actual harm is not pled.[48]

D. *How Stolen Data Is Monetized—The "Dark Web"*[49]

In most cases of data breach, criminals will seek to monetize data using illegal means.[50] When personal information is stolen through data breaches, the victims begin to be proactively protective of their information. Victims employ credit-checking safeguards, complex dark web scans, and a host of other defensive mechanisms to try to protect their identities—however the cyber-sleuths that plunder major corporations are patient.

Stolen data can be held by thieves for years and then uploaded onto dark web message boards that function as an online sales site. To understand how this process works, an understanding of the functionality of the internet is necessary. The internet is effectively broken up into three layers. The first layer is the "surface web," which is the web interface most users are familiar with when using a popular web search browser, such as Google or Yahoo.[51] However, there is a more secretive part of the internet that most users unwittingly encounter. This second layer is called the "deep web."[52] This portion of the internet can be categorized as anything that search engines do not catalog.[53] When users log in to check their bank balance, they have entered the deep web. When users log into a secure database, such as Westlaw or LexisNexis, they have also entered the deep web. These websites have been coded to prevent access from the web crawlers that search engines use to index the internet.[54]

---

48. *See, e.g.*, Urman v. S. Bos. Sav. Bank, 674 N.E.2d 1078, 1083 (Mass. 1997) (holding that the threat of future harm is not recoverable as tort damages).

49. The Authors have decided to limit the scope of their explanation of how data is stolen and monetized on the "dark web" to avoid creating a "how-to" guide for would-be nefarious readers.

50. *See generally Data Thieves: Hearing Before the Subcomm. on Terrorism and Illicit Fin. of the H. Comm. on Fin. Servs.*, 115th Cong. (2018) (statement of Lillian Ablon, Information Scientist, The RAND Corporation), available at https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf [https://perma.cc/AWL2-RKKU] [hereinafter *Data Thieves*] (explaining the different types of actors and how they steal and monetize data).

51. *Definition of: Surface Web*, PC, https://www.pcmag.com/encyclopedia/term/52273/surface-web [https://perma.cc/Y2G7-JUYH].

52. *Definition of: Deep Web*, PC, https://www.pcmag.com/encyclopedia/term/41069/deep-web [https://perma.cc/4SRP-8EUR].

53. *See id.*

54. *See id.*

Below the deep web is the so-called "dark web"—the third and final layer of the internet. This is the portion of the internet used by hackers, drug dealers, and internet scammers.[55] The dark web has forums that allow members to discuss strategies and provide effective tutorials for others starting in the world of hacking. It also has marketplaces dedicated to buying and selling software, counterfeit currency, drugs, and—of course—identities,[56] which can range from hacked accounts to forged passports. While these offerings may not be entirely verifiable within legal means, they are relatively easy to find. To access these "dark" corners of the internet, one needs only the right internet browser.

The Onion Routing Project, commonly known as Tor, is the most commonly used browser to access the dark web.[57] It works much like any other internet browser, but instead of relaying one's request directly to the website server, it sends a user's connection through a vast network of volunteer servers to disguise where the request came from and where it is going. This allows some degree of anonymity while browsing the web.[58] Tor also encrypts all transmissions, so even if one's browsing was discovered, it would need to be decrypted to be understood.[59]

Tor is often used for political dissidents in totalitarian regimes.[60] Specifically, in Tor, there are many tools and websites with a dedicated purpose of allowing whistle-blowers to disseminate classified information directly to reporters.[61] The encryption system also allows users to browse more privately than traditional internet browsers.[62] The Navy uses Tor for intelligence gathering, and law enforcement agencies use it for surveillance and sting operations.[63] In fact, the Tor project was originally created by the U.S. Naval Research Laboratory to protect U.S. intelligence

55. *See Definition of: Dark Web*, PC, https://www.pcmag.com/encyclopedia/term/67980/dark-web [https://perma.cc/WX9P-X88H].

56. *See* Max Eddy, *Inside the Dark Web*, PC (Feb. 4, 2015, 8:00 AM), https://www.pcmag.com/article/331580/inside-the-dark-web [https://perma.cc/T3PZ-EQS4].

57. *See generally About: History*, TOR, https://www.torproject.org/about/history/ [https://perma.cc/AWM6-YG49].

58. *See id.*

59. *Id.* ("The goal of onion routing was to have a way to use the internet with as much privacy as possible, and the idea was to route traffic through multiple servers and encrypt it each step of the way.").

60. Alkira Reinfrank, *What is the 'Dark Web'? Term Made Famous by Ashley Madison and Paedophile Rings Explained*, ABC: NEWS (Aug. 28, 2015, 12:54 AM), https://www.abc.net.au/news/2015-08-27/dark-web-dark-net-deep-web-paedophiles/6729916 [https://perma.cc/ANY8-6X8C].

61. *See id.*

62. *See id.*

63. *Id.*

communications on the internet.[64] The Tor project is still largely funded by the United States Federal Government and has extremely important and legitimate uses.[65]

However, it is still the last place one would want his or her personal information to end up. With hacking tutorials and networks of illegal marketplaces, data breaches can lead to the theft and sale of thousands of users' information before the user even notices. Credit companies, therefore, have started programs to "scan" the dark web for individuals information.[66] You may have seen commercials advertising a security company's ability to monitor the dark web for individuals' social security numbers. While these safeguards exist, websites on the dark web come into and out of existence faster than can be tracked, and many of these websites sell services like stolen data and identities.[67]

To understand the specific steps hackers take to monetize stolen data, an excerpt from the article, *Once Stolen, What Do Hackers Do With Your Data?*, concisely discusses the process as follows:

> Once an attack has happened and the criminal has your data, he or she likely runs through the following steps, which we like to call, "A Hacker's Post Breach Checklist:"
>
> 1. Inventory the stolen data—Hackers will look through the stolen data files for authentication credentials, personal information like names, addresses and phone numbers, and financial information like credit card details.
>
> 2. Sell personal information—Next, the hacker will package up personal information like names, addresses, phone numbers, and email addresses and sell them, typically in bulk. These are more valuable the more recent they are. According to Quartz, a full set of someone's personal information including identification number, address, birthdate, and possibly credit card info costs between $1 and $450 with a media[n] cost of $21.35.
>
> 3. Look for the good stuff—Hackers will then inventory authentication credentials further and look for potentially lucrative accounts. Government and military addresses are very valuable, as well as company email addresses and passwords for large corporations. Since people often re-use their passwords, hackers can

64. JOSEPH BABATUNDE FAGOYINBO, THE ARMED FORCES: INSTRUMENT OF PEACE, STRENGTH, DEVELOPMENT AND PROSPERITY 262 (2013).

65. *See* Yasha Levine, *Almost Everyone Involved in Developing Tor Was (or Is) Funded by the US Government*, PANDO (July 16, 2014), https://pando.com/2014/07/16/tor-spooks/ [https://perma.cc/63L9-MJ6A].

66. *See, e.g.*, *Is Your Information on the Dark Web?*, EXPERIAN, https://www.experian.com/consumer-products/free-dark-web-email-scan.html [https://perma.cc/34XB-WJUW].

67. *See Data Thieves*, *supra* note 50, at 1.

> often use credentials for military or corporate accounts to target other companies. For example, Dropbox was breached in 2012 using credentials stolen in the LinkedIn data breach earlier that year. A hacker may plan such a hack himself, or he/she may sell the credentials to others on the dark web for a much higher price.
>
> 4. Offload the cards—Financial information like credit card numbers are packaged and sold in bundles. An individual with the right knowledge could easily buy credit card information in groups of ten or a hundred. Usually, a "broker" buys the card information, then sells them to a "carder" who goes through a shell game of purchases to avoid being detected. First the "carders" use stolen credit card [sic] to buy gift cards to stores or to Amazon.com, then use those cards to buy physical items. The carder may then sell the electronics through legitimate channels like eBay, or through an underground dark website.
>
> 5. Sell in bulk—After several months, the hacker will bundle up authentication credentials and sell them in bulk at a discounted price. By now, most of the credentials are worthless since the company has most likely discovered the breach and taken steps to repair it. For example, a database containing the entire LinkedIn credentials dump is still available.[68]

E. *The Significance of Data Theft*

Data theft touches many industries, and the cost of the losses continues to rise. The *2018 Cost of Data Breach Study* found that the average cost for each lost record is on the rise.[69] The highest costs resulting from lost or stolen records were health care related data.[70] In 2017, sixteen large breaches occurred, which is much higher than the nine large breaches that occurred just four years previously in 2013.[71] The study also confirmed what many believe to be obvious—the larger the breach, the higher the cost.[72] After significant study, the Ponemon Institute made several findings regarding data breaches. Specifically the Institute found that most breaches were caused by "malicious and criminal attacks" as opposed to human error, and it took, on average, 266 days from

68. The Editor, *Once Stolen, What Do Hackers Do With Your Data?*, SECPLICITY (May 18, 2017), https://www.secplicity.org/2017/05/18/stolen-hackers-data/ [https://perma.cc/X26J-D8HS].

69. PONEMON INST., LLC, 2018 COST OF A DATA BREACH STUDY: GLOBAL OVERVIEW 3–4 (2018), https://www.ibm.com/downloads/cas/861MNWN2 [https://perma.cc/ZV6H-QW6V].

70. *Id.* at 18 fig.7.

71. *See generally* PONEMON INST., LLC, 2013 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS (2013), https://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf [https://perma.cc/FZT2-NALN].

72. *See* PONEMON INST., LLC, *supra* note 69, at 39.

detection of the breach to containment.[73] In addition, those breaches that affected one million records cost the company about $40 million dollars, whereas a breach involving 50 million records cost the company approximately $350 million dollars.[74]

II. EXISTING DATA PROTECTION LAWS AND REGULATIONS—A PATCHWORK OF UNORGANIZED REMEDIES

Although a comprehensive national data protection law that provides individual consumers with rights and remedies against negligent data holders would be ideal, consumers are currently forced to navigate their way through a patchwork of various state and federal laws that ultimately provide limited protection. A survey of existing data protection laws follows.

A. *Federal Data Protection Laws*

Surprisingly, unlike recent significant data protection legislation in Europe,[75] a comprehensive federal privacy law in the United States is lacking. Although Congress has contemplated nationalized legislation that would create a uniform system of data regulation, legislation has failed to pass thus far.[76] As such, state and local lawmakers have been forced to try and tackle this exceptionally complex issue. However, as the participants in the crime are often located in different states (and sometimes countries), the effectiveness of local laws is minimized. In response, industry groups have also attempted to address the issue by agreeing on guidelines and best practices and urging the U.S. Congress to adopt a federal standard.[77] Although these mechanisms do not have the force of law, they are at least an attempt to voluntary achieve compliance with heightened data protection within various industries.

The federal privacy-related laws that do regulate the collection and use of personal data are fragmented, and each law primarily pertains to a particular sector of industry, including: (i) laws that regulate consumer

73. *Id.* at 4, 19–21.

74. *Id.* at 4.

75. *See generally* Griffin Drake, Note, *Navigating the Atlantic: Understanding EU Data Privacy Compliance Amidst a Sea of Uncertainty*, 91 S. CAL. L. REV. 163 (2017) (providing a robust discussion of the EU General Data Protection Regulation).

76. *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/LH63-9P7K].

77. Danielle Abril, *This is What Tech Companies Want in Any Federal Data Privacy Legislation*, FORTUNE (Feb. 21, 2019), http://fortune.com/2019/02/21/technology-companies-federal-data-privacy-law/ [https://perma.cc/NZ63-MEE4].

data maintained by insurance and financial institutions;[78] (ii) laws that regulate consumer data maintained by medical and other healthcare providers;[79] and (iii) laws that regulate consumer data maintained by telecommunication companies, including those that telemarket and engage in commercial e-mail.[80] Furthermore, consumer protection laws designed to prohibit unfair and deceptive commercial practices are being used to hold companies accountable.[81]

The Federal Trade Commission Act (FTCA)[82] is a broad federal consumer protection law that holds businesses accountable for "unfair or deceptive acts or practices."[83] The FTCA, initially enacted in 1914,[84] has more recently been applied to policies surrounding privacy and data security.[85] Companies that fail to adequately safeguard personal information and data have been subject to Federal Trade Commission (FTC) investigation and prosecution.[86] For example, in *FTC v. Wyndham Worldwide Corp.*, due to unfair and deceptive practices, the FTC sued a hotel chain for failing to adequately safeguard their customers' personal information.[87] In first addressing a jurisdictional issue, the court held the FTC, under the FTCA's prohibition against unfair and deceptive acts and practices, had authority to regulate companies failing to ensure that their consumers' personal information was reasonably and appropriately secured, even though Congress had enacted other statutes that concerned data security.[88] In addition, the FTC's authority over data security could coexist with existing data-security regulatory schemes.[89]

Equally important to safeguarding against unfair and deceptive acts, the FTC also ensures compliance with the Children's Online Privacy Protection Act (COPPA),[90] which regulates the collection of data and

78. Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2018).

79. Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d-6 (2018).

80. *See* Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–09 (2018).

81. *See* In re Anthem, Inc. Data Breach Litigation, 162 F. Supp. 3d 953, 990 (N.D. Cal. 2016) (utilizing the FTCA, a consumer protection law, in a case arising out of a data breach).

82. 15 U.S.C. §§ 41–58.

83. *Id.* § 45(a)(1).

84. *See* Marc Winerman, *The Origins of the FTC: Concentration, Cooperation, Control, and Competition*, 71 ANTITRUST L.J. 1, 2 (2003) (noting the passage of the FTCA in 1914).

85. *See In re Anthem, Inc.*, 162 F. Supp. 3d at 990 (applying the FTC to a data breach claim).

86. *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 259 (3d Cir. 2015) (holding that Wyndham had violated the law by failing to safeguard user information).

87. *Id.* at 240–41.

88. *See id.* at 243–49.

89. *See id.* at 248.

90. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2018).

information from children. It is also important to note that the FTCA does not allow for a private cause of action.[91]

The Financial Services Modernization Act,[92] otherwise known as the Gramm-Leach-Bliley Act (GLBA), was primarily drafted to allow companies from different financial industries, such as banks, insurance companies, and securities firms to merge.[93] However, the GLBA also contains some important components regarding the collection, use, and disclosure of financial information. Specifically, non-public personal information is regulated and limited.[94] In addition, financial institutions are required to notify customers of their privacy practices and give customers an opportunity to opt out of having some of their information shared.[95] Although a significant and powerful regulation, the GLBA, unfortunately, provides no private cause of action recognized by courts.[96]

The Health Insurance Portability and Accountability Act (HIPAA) regulates medical information and is applied broadly to a variety of entities that encounter medical information, which encompasses health care providers, data processors, and pharmacies.[97] HIPAA was drafted

---

91. 15 U.S.C.A. § 45(n). *See generally* Jeff Sovern, *Private Actions Under the Deceptive Trade Practices Acts: Reconsidering the FTC Act as Rule Model*, 52 OHIO ST. L.J. 437 (1991) (discussing private causes of action created by state law, their benefits, drawbacks, and foundation in the FTCA).

92. Financial Services Modernization Act, 15 U.S.C. §§ 6801–6809; 6821–6827 (2018) (containing sections of the Financial Services Modernization Act, also referred to as the Gramm-Leach-Bliley Act).

93. *See* Joe Mahon, *Financial Services Modernization Act of 1999, Commonly Called Gramm-Leach-Bliley*, FED. RES. HIST. (Nov. 12, 1999), https://www.federalreservehistory.org/essays/gramm_leach_bliley_act [https://perma.cc/VXB4-PXJY] (discussing the impact of the repeal of Glass-Stegall on the allowance of mergers).

94. 15 U.S.C. § 6802(a).

95. *Id.*

96. *See In re* French, 401 B.R. 295, 309 (Bankr. E.D. Tenn. 2009). In *French*, a bankruptcy debtor's social security number and date of birth were improperly included on a proof of claim filed by a creditor. As this information becomes publicly available once the proof of claim is filed, the debtor brought an action against the creditor for a variety of claims, including violation of the Gramm-Leach-Bliley Financial Modernization Act. Following the creditor's motion to dismiss, the court declared: "By its very terms, the Gramm-Leach-Bliley Act does not provide a private right of action." *Id.* at 310 (citing Dunmire v. Morgan Stanley DW, Inc., 475 F.3d 956, 960 (8th Cir. 2007) ("No private right of action exists for an alleged violation of the GLBA."); Farley v. Williams, No. 02-CV-0667C(SR), 2005 WL 3579060, at *3 (W.D.N.Y. Dec. 30, 2005) ("[A] private right of action does not exist on behalf of an individual . . . claiming harm as the result of a financial institution's failure to comply with the GLBA's privacy provisions."); Southhall v. Check Depot, Inc., No. 07-001115-TOM-13, 2008 WL 5330001, at *4 (Bankr. N.D. Ala., Dec. 19, 2008) ("Courts have consistently held that there is no private cause of action created by Congress in the GLBA.")).

97. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of title 18, 26, 29, and 42 of the U.S.C.).

broadly and covers many aspects of consumer privacy. The Standards for Privacy of Individually Identifiable Health Information regulate the storage and use of protected health information.[98] The Security Rule provides standards for protecting medical data.[99] The Standards for Electronic Transactions applies to the electronic transmission of medical data.[100] Although HIPPA creates an expansive list of protections, again, no private cause of action exists for an individual to bring suit for violation of the statute.[101]

Despite the lack of a private cause of action for claims filed under HIPPA, the majority of courts that have considered the privacy issue have concluded that there is a common law duty of confidentiality arising from the physician-patient relationship.[102] Courts have relied on the fact that there was a public policy justification arising out of the duty of confidentiality between a patient and physician.[103] Other courts have held

---

98. *See Standards for Privacy of Individually Identifiable Health Information*, OFF. ASSISTANT SECRETARY FOR PLAN. & EVALUATION (July 6, 2001), https://aspe.hhs.gov/standards-privacy-individually-identifiable-health-information [https://perma.cc/Q7PJ-WFHB] [hereinafter *Standards for Privacy*].

99. *See The Security Rule*, U.S. DEP'T. HEALTH & HUM. SERVICES (May 12, 2017), https://www.hhs.gov/hipaa/for-professionals/security/index.html [https://perma.cc/GX4N-2PCE].

100. 45 C.F.R. §§ 162.1601–03 (2000); *Standards for Privacy*, *supra* note 98.

101. Acara v. Banks, 470 F.3d 569, 572 (5th Cir. 2006). In *Acara*, the plaintiff sued their doctor for violating HIPPA after disclosing unauthorized information during a deposition. *Id.* at 570. When evaluating if a federal statute provides a private cause of action, the court must evaluate the intent of language of the statute. The court held that

> [w]hile no other circuit court has specifically addressed this issue, we are not alone in our conclusion that Congress did not intend for private enforcement of HIPAA. Every district court that has considered this issue is in agreement that the statute does not support a private right of action.
>
> Furthermore, Acara provides no authority to support her assertion that a private right of action exists under HIPAA, and her policy arguments are unpersuasive. We hold there is no private cause of action under HIPAA and therefore no federal subject matter jurisdiction over Acara's asserted claims.

Id. at 571–72 (citations omitted).

102. *See, e.g.*, Brandt v. Med. Def. Assocs., 856 S.W.2d 667, 669–71 (Mo. 1993) (explaining the duty of confidentiality owed to a patient by a physician).

103. *See* Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 175 A.3d 1, 7 (Conn. 2018); *see also* Alberts v. Devine, 479 N.E.2d 113, 119 (Mass. 1985) ("The courts that have imposed on physicians a duty of confidentiality and have recognized a cause of action to enforce that duty have grounded their decisions on the determination that public policy favors the protection of a patient's right to confidentiality."); Aufrichtig v. Lowell, 650 N.E.2d 401, 404 (N.Y. 1995); McCormick v. England, 494 S.E.2d 431, 439 (S.C. Ct. App. 1997).

> [T]he [l]egislature has demonstrated its recognition of a policy favoring confidentiality of medical facts by enacting [statutes] . . . to limit the availability of hospital records. Furthermore, [the legislature has also] create[d] an evidentiary privilege as to confidential communications between a psychotherapist and a patient. The fact that no such statutory privilege obtains with respect to physicians generally and their patients does not dissuade us from declaring that in this

that state common law causes of action compliment HIPAA.[104] A minority of courts, however, have refused to recognize a cause of action for the breach of a confidential or privileged relationship in the absence of statutory authority.[105]

Both consumer reporting agencies and agencies providing consumer-reporting information (including lenders and credit card companies) are accountable for user privacy under The Fair Credit Reporting Act and the Fair and Accurate Credit Transactions Act—which amended the Fair Credit Reporting Act.[106] Consumer reports are the

> communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal

---

> Commonwealth all physicians owe their patients a duty, for violation of which the law provides a remedy, not to disclose without the patient's consent medical information about the patient, except to meet a serious danger to the patient or to others.

Alberts v. Devine, 479 N.E.2d at 119 (citation omitted).

104. Crescenzo v. Crane, 796 A.2d 283, 284–85 (N.J. Super. Ct. App. Div. 2002) (allowing the plaintiff's complaint to proceed against her physician when he responded to a subpoena by disclosing medical records without notice or authorization in violation of common law); *see* Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 523 (Ohio 1999) ("[A]n independent tort exists for the unauthorized, unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship."); *see also* Sorensen v. Barbuto, 143 P.3d 295, 300 (Utah Ct. App. 2006) ("[E]x parte communication between a physician and opposing counsel constitutes a breach of the physician's fiduciary duty of confidentiality."). The *Sorenson* court further determined that "the trial court erred in dismissing [the plaintiff's] claim for breach of confidentiality" and "determin[ing] that a duty exists, [ruled that] the trial court [also] erred in dismissing [the plaintiff's] claim for negligence." *Id.* at 301.

105. Mikel v. Abrams, 541 F. Supp. 591, 599 (W.D. Mo. 1982) (refusing to follow cases from other states and declining to recognize cause of action for breach of confidential or privileged relationship because no Missouri case had recognized a cause of action before), *aff'd*, 716 F.2d 907 (8th Cir. 1983); Collins v. Howard, 156 F. Supp. 322, 324 (S.D. Ga. 1957) (citation omitted) ("There is no confidential relationship between doctor and patient or hospital and patient in Georgia."); Quarles v. Sutherland, 389 S.W.2d 249, 251–52 (Tenn. 1965) (declining to recognize cause of action for breach of confidentiality where state had no common-law or statutory privilege for communications between patient and physician); *see* Logan v. District of Columbia, 447 F. Supp. 1328, 1335 (D.D.C. 1978). In *Logan*, the court held:

> Other jurisdictions have recognized a cause of action for unauthorized disclosure of information obtained through the physician-patient relationship. The plaintiff, however, has not persuaded this court that such a cause of action should or would be recognized by the courts of this jurisdiction. Further, the plaintiff's invasion of privacy action is sufficient to redress any breach of the confidentiality of the physician-patient relationship.

Id.

106. Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (2018); Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (amending §§ 1681–1681x).

> characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance . . . .[107]

B. *Other Law and Guidelines*

When the personal information of certain allied-nation foreign citizens was improperly shared with law enforcement, Congress enacted redress in 2016 under the Judicial Redress Act.[108] Further, there are many other federal information security and enforcement laws governing the use and control of personal information.[109]

In addition to statutory laws, various industry groups (such as the payment cards, mobile marketing, and online advertising industries) have issued guidelines for their members based on best practices for their respective industries.[110] Some industry groups, such as the advertising industry, have worked to develop their own rules for online advertising.[111] Essentially, this industry agreement requires cooperating members to

---

107. 15 U.S.C. § 1681a(d)(1)(A) (2018); *see* Longman v. Wachovia Bank, N.A., 702 F.3d 148, 149–50 (2nd Cir. 2012). In *Longman*, the plaintiff filed an action against Wachovia for violating the Fair Credit Reporting Act by making false reports to credit reporting agencies, and then failing to correct them after being told of the discrepancy by the consumer. The court held:

> Although we have not previously addressed whether the Fair Credit Reporting Act provides a private cause of action for violations of § 1681s–2(a), the statute plainly restricts enforcement of that provision to federal and state authorities. Indeed, the statute provides that subsection (a) "shall be enforced *exclusively* . . . by the Federal agencies and officials and the State officials identified in section 1681s of this title." Thus, the district court correctly concluded, as many other courts have held, that there is no private cause of action for violations of § 1681s–2(a).

Id. at 151 (citations omitted).

108. Judicial Redress Act, 5 U.S.C. § 552 (2018).

109. *See, e.g.*, 15 U.S.C. § 1681 (2018); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2018); Gramm-Leach-Bliley Act, 15 U.S.C. § 6802(a) (2018); CAN-SPAM Act 15 U.S.C. § 7704 (2018); Video Privacy Protection Act, 18 U.S.C. § 2710 (2018); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2018); Health Information Portability and Accountability Act, 29 U.S.C. § 1181 (2018); Telephone Consumer Protection Act, 47 U.S.C. § 227 (2018).

110. For example, The Payment Card Industry Security Standards Council mandates that credit card members comply with the Payment Card Industry Data Security Standard to reduce fraud. *See About Us*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/about_us/ [https://perma.cc/84TQ-PVRB]. The International Association for Healthcare Security and Safety implemented guidelines that members must comply with in order to promote security. *See About Us*, INT'L ASS'N FOR HEALTHCARE SECURITY & SAFETY, https://www.iahss.org/page/aboutus [https://perma.cc/J5JH-TMN6].

111. *See Self-Regulatory Program for Online Behavioral Advertising Factsheet*, IAB, https://www.iab.com/wp-content/uploads/2015/06/OBA_OneSheet_Final.pdf [https://perma.cc/62MU-46FP].

comply with group guidelines that resemble those of the FTC.[112] Those industry members who comply with the voluntary guidelines are able to use a symbol on their advertisements to let others know they are compliant.[113]

1. European Data Regulation

The General Data Protection Regulation (GDPR) was finally implemented in May 2018.[114] It was one of the first major sweeping attempts at regulating European Union companies' use of data that previously had been able to use consumers' data with little restriction.[115] The GDPR is both broad in scope and deep in substance. It provides significant protection for European consumers.[116] Under the GDPR, if companies operating under its jurisdiction do not report security breaches to the government and consumers within seventy-two hours of becoming aware of the breach, or hold data for longer than is necessary, the company can face significant financial penalties.[117] Specifically, the GDPR imposes the following restrictions and remedies on European companies:

- *Imposition of Significant Penalties*. Organizations in breach of GDPR can be fined up to twenty million euros or four percent of annual global turnover (whichever is greater).[118]
- *Consumer Consent*. When requesting data from a consumer, the request must include a request for consent in a simple and easily accessible form that explains the purpose for the data requested. The GDPR specifically states that the consent must use clear and

112. *See id.*

113. *See id.*

114. *See A New Era for Data Protection in the EU*, EUR. COMMISSION, https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf [https://perma.cc/7N9V-FSCA].

115. *See generally* Council Regulation 2016/679, 2016 O.J. (L 119). In describing the underlying principle of the law, the regulation defines data protection as follows:

> The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

Id. at 2.

116. *See id.* at 1–2.

117. *See id.* at 52, art. 33(1).

118. *Id.* at 83, art. 83(6).

plain language and be distinguishable from other consent requests being simultaneously made. Under GDPR, the consumer maintains the right to withdraw consent at any time.[119]

- *Consumer Notification of Data Breach*. Under the GDPR, breach notifications are mandatory and must be done within 72 hours of the company first having become aware of the breach, and data processors are also required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.[120]
- *Consumer's Right to be "Forgotten"*. In addition to the right to know what their data is being used for, and an ongoing right to access the data, the GDPR also entitles an individual to have their personal data forgotten (i.e., erased), and to prevent further dissemination.[121]
- *Privacy by Design*. In a very forward-thinking move, the GDPR requires inclusion of data protection safeguards from the onset of designing systems that collect data. More specifically, "the controller shall . . . implement appropriate technical and organisational measures . . . in an effective manner . . . in order to meet the requirements of this Regulation and protect the rights of data subjects."[122]

What is more important, the GDPR establishes a private right of action.[123] Article 80(1) provides that "[t]he data subject shall have the right to mandate a not-for-profit body, organization or association . . . to lodge the complaint on his or her behalf."[124]

2. State Privacy Laws

States have taken the lead on laws that regulate personal data use and collection, with the number growing annually.[125]

> Some federal privacy laws pre-empt state privacy laws on the same topic. For example, the federal law regulating commercial e-mail and the sharing of e-mail addresses pre-empts most state laws regulating the same activities. Conversely, there are many federal privacy laws that do not pre-empt state laws, which means that a company can find

119. *Id.* at 37, art. 7.
120. *Id.* at 52–53, art. 33–34.
121. *Id.* at 43–44, art. 17.
122. *Id.* at 48, art. 25(1).
123. *Id.* at 81, art. 82(1).
124. *Id.* art. 80(1).
125. *See* Jeewon Kim Serrato et al., *US States Pass Data Protection Laws on the Heels of the GDPR*, NORTON ROSE FULBRIGHT: DATA PROTECTION REP. (July 9, 2018), https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/ [https://perma.cc/8WZ6-97LG].

> itself in the position of trying to comply with federal and state privacy laws that regulate the same types of data (for example, medical or health records) or [the same] types of activit[ies].[126]

As the federal government has failed to act in a comprehensive manner that empowers consumers, states have taken it upon themselves to close the gap with their own legislation. Although state consumer protection legislation is often broadly written, it is also important to recognize the limited jurisdiction to which it applies, in that it only impacts business within that state. California and Massachusetts are examined below as examples of states that have legislated to close the federal consumer protection loopholes.

a. State law remedies—California data breach notification laws

In response to the significant role technology plays in California's economy, California has lead the nation in recognizing and protecting consumer privacy by enacting the first data-breach notification law.[127] As the first state to enact a security breach notification law, California law requires disclosure of any breach by any business "that owns or licenses computerized data that includes personal information."[128] The disclosure must be made to all California residents "whose unencrypted personal information was . . . acquired by an unauthorized person."[129]

Following California's lead, many other states adopted laws that were similar to California and required disclosure of a breach to in-state residents.[130] Although consumer notification is important, a criticism of

---

126. *Sources of U.S. Data Privacy Law*, LEGITIMIS (Sept. 18, 2016), http://www.legitimis.de/en/sources-of-u-s-data-privacy-law/ [https://perma.cc/4J8J-M3JY]; *see also* CAN-SPAM Act, 15 U.S.C. § 7707(b) (2018); Peter Swire, *US Federal Privacy Preemption Part 1: History of Federal Preemption of Stricter State Laws*, IAPP (Jan. 9, 2019), https://iapp.org/news/a/us-federal-privacy-preemption-part-1-history-of-federal-preemption-of-stricter-state-laws/ [https://perma.cc/8WKU-4EJ3] (discussing the fact that that three federal privacy statutes have provisions regarding pre-emption, including CAN-SPAM, Fair Credit Reporting Act, and COPPA).

127. *See* O'Connor, *supra* note 76.

128. CAL. CIV. CODE § 1798.82(a) (West 2019); *see also* Forbes Tech. Council, *How Will California's Consumer Privacy Law Impact the Data Privacy Landscape?*, FORBES (Aug. 20, 2018, 9:30 AM), https://www.forbes.com/sites/forbestechcouncil/2018/08/20/how-will-californias-consumer-privacy-law-impact-the-data-privacy-landscape/#663c3eaee922 [https://perma.cc/4LJT-THKT].

129. The California statute includes an exception for law enforcement. Specifically, it states, "[t]he notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation." § 1798.82(c).

130. *See* Serrato et al., *supra* note 125.

this approach is that it is reactive as opposed to proactive, only requiring action after a breach has occurred.[131]

Beyond simple notification, California also sought to significantly restrict access to private data through the California Electronic Communications Privacy Act,[132] which limits the ability of government authorities to seek electronic communication information for law enforcement purposes.[133]

More recently, in July of 2018, California passed the broadest of privacy laws in the United States and picked up on several of the protections put forth by the European Union's GDPR.[134] The California Consumer Privacy Act of 2018 (effective January 2020), will provide consumers with new rights, including the right to require the deletion of their data and request disclosures about how information is collected and shared. Consumers can also direct a data holder specifically not to sell their data without additional consent, and upon enactment, individuals will have a private right of action to pursue violators after the January 2020 effective date.[135]

b. Massachusetts data protection laws

Similar to California, Massachusetts has always been on the forefront of consumer protection rights. Looking to both define and prevent data security breaches, Massachusetts enacted a regulation which provides an extensive "list of technical, physical and administrative security protocols aimed at protecting personal information."[136] In addition, these

131. *See* 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, 483 (2010) (critiquing notification laws).

132. *See generally* California Electronic Communications Privacy Act, 2015 Cal. Legis. Serv. Ch. 651 (West) (codified at CAL. PENAL CODE §§ 1546–46.4 (West 2019)).

133. Some of the limitations of the California Electronic Communications Privacy Act include S.B. 570, which amends the required content of security breach notices, requiring that notices clearly and conspicuously display certain prescribed headings. S.B. 570, 2015–16 Leg., Reg. Sess. (Ca. 2015). California's legislature now defines the term "encrypted" for purposes of California's breach notification law as "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information technology." A.B. 964, 2015–16 Leg., Reg. Sess. (Ca. 2015).

134. *See supra* Section II.B.1.

135. California Consumer Privacy Act, 2017–18 Leg., Reg. Sess. (Ca. 2018) (S.B. 1121) (codified as amended at CAL. CIV. CODE §§ 1978.100–78.199) (effective Jan. 1, 2020).

136. Julie DiMauro, *Checklist of Data Protection Best Practices*, THOMSON REUTERS: REG. INTELLIGENCE (Mar. 15, 2016), https://blogs.thomsonreuters.com/answerson/data-protection-action-items-for-firms/ [https://perma.cc/K2RC-PCWN]. *See generally* Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 MASS. CODE REGS. 17.01–17.05 (2019).

Massachusetts companies must take a proactive stance and implement the requirements of Title 201 of the Code of Massachusetts Regulations, also known as the Massachusetts Data Security Regulations, into their existing data security programs.[137]

The Massachusetts Data Security Regulations instruct data holders how to both limit and prevent data breach and also instruct the data holder as to what they must do when a breach happens.[138] Specifically, the law states:

> If you know or have reason to know that your organization has experienced a data breach covered by the Breach Notification Law, you must [then comply with the Breach Notification Law and] send written notices as soon as practicable and without unreasonable delay, to: [t]he Attorney General's Office; [t]he Office of Consumer Affairs and Business Regulation; and [t]he affected Massachusetts residents . . . .[139]

This regulation implements the provisions of Chapter 93H of the Massachusetts General Laws, which applies to those who possess (either through ownership or lease) personal data of Massachusetts residents.[140] The statute also states the minimum requirements necessary to safeguard the data.[141] The objectives of this regulation are to "ensure the security and confidentiality of customer information in a manner fully consistent with industry standards."[142] Accordingly, this regulation seeks to "protect against anticipated threats or hazards to the security or integrity of such information[,] and to protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer."[143] In this context, the term breach is defined by the Massachusetts Data Security Regulations as follows:

> [T]he unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident

137. *See* 201 MASS. CODE REGS. 17.03 (2019).

138. *See* 201 MASS. CODE REGS. 17.03–17.04 (2019).

139. *Obligations Under the Data Security Regulations and Breach Notification Law*, MASS.GOV, https://www.mass.gov/service-details/obligations-under-the-data-security-regulations-and-breach-notification-law [https://perma.cc/T9AC-RCUV]; *see* MASS. GEN. LAWS ch. 93H, § 3 (2018).

140. *See* MASS. GEN. LAWS ch. 93H, § 2(a) (2018).

141. *See id.*

142. *Id.* § 2.

143. *Id.*

> of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.[144]

Commonwealth v. Equifax, Inc. involved an action brought after Equifax, Inc suffered a significant data breach that exposed "millions of people's data to unauthorized third parties."[145] Equifax is a credit reporting agency that collects and stores consumer data for purposes of selling credit reports and credit scores.[146] In 2017, third party hackers took advantage of a flaw in Equifax's computer code, thus allowing the thieves to steal millions of people's personal data, including credit card numbers, dates or birth, and driver's license numbers.[147]

The Massachusetts Attorney General brought suit against Equifax for their failure to safeguard the personal information of Massachusetts residents when their databases were breached, and subsequently failing to notify these consumers when said breach occurred.[148] The attorney general was able to convince the court to not dismiss the complaint.[149] Had the attorney general decided not to pursue this matter against Equifax, it is uncertain if a private individual would have had standing to do so.

---

144. 201 MASS. CODE REGS. 17.02 (2019).

145. Commonwealth v. Equifax, Inc., No. 1784CV03009BLS2, 2018 WL 3013918, at *1 (Mass. Super. Ct., Apr. 3, 2018).

146. *See* Geoff Williams, *What Is Equifax and Why Does It Have My Financial Information?*, U.S. NEWS & WORLD REP.: MONEY (Sept. 19, 2017, 10:03 AM), https://money.usnews.com/money/personal-finance/banking-and-credit/articles/2017-09-19/what-is-equifax-and-why-does-it-have-my-financial-information.

147. *See* Erica R. Hendry, *How the Equifax Hack Happened, According to Its CEO*, PBS NEWS HOUR (Oct. 3, 2017, 9:43 AM), https://www.pbs.org/newshour/nation/equifax-hack-happened-according-ceo [https://perma.cc/D3VR-HKKK].

148. *Equifax, Inc.*, 2018 WL 3013918, at *1.

149. *Id.* Interestingly, Equifax attempted to dismiss the action based on the fact the Commonwealth of Massachusetts had failed to prove any actual harm had occurred as a result of the breach. In dismissing this argument, the court held:

> This argument fails because the Attorney General, unlike a private litigant who sues under § 9 or § 11 of c[h]. 93A, is only required to prove that unfair or deceptive acts or practice took place in trade or commerce; she is not required to prove or quantify resulting economic injury. The Attorney General may seek injunctive relief or civil penalties "[w]henever" she "has reason to believe that any person is using or is about to use" an unfair or deceptive act or practice in violation of the consumer protection act.

Id. at *5 (second alteration in original) (quoting ch. 93A, § 4). The court went on to say "[the Attorney General] is not required to allege or prove that any individual consumer was actually harmed by the allegedly unfair or deceptive act or practice." *Id.* (citing Commonwealth v. Fall River Motor Sales, Inc., 565 N.E.2d 1205, 1212 (Mass. 1991); Commonwealth v. Chatham Dev. Co., 731 N.E.2d 89, 91–92 (Mass. App. Ct. 2000)).

Despite the proactive data security protocols, if a breach does occur, Massachusetts, like California, requires consumer notification pursuant to Massachusetts General Law chapter 93H. Specifically, 93H states:

> A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor in accordance with this chapter.[150]

The difficulty of trying to use state law to remedy theft of an individual's data is the enforcement of the law. Much like their federal statutory counterparts, many of the protections created in the state statutes and regulations are only enforceable through government actors, not individual victims.[151] This leaves the decision to pursue redress solely to the state. Thus, decisions to bring an action (or to not bring an action) can easily be influenced by the availability of state resources, arbitrary decisions regarding the seriousness of the breach, and even politics depending on who the wrongdoer may be.[152] For example, under chapter 93H (discussed above), only the Massachusetts Attorney General is expressly granted authority to bring suit for enforcement.[153]

In *Aminpour v. Arbella Mutual Insurance Co.*, the plaintiff (an individual homeowner) brought suit against her homeowner's insurance carrier for various claims, including violation of chapter 93H.[154] Without evaluating the merits of the security breach claim, the lower court dismissed the chapter 93H claim based on lack of standing as the attorney general had not taken any action.[155] Unfortunately, based on the express

---

150. MASS. GEN. LAWS ch. 93H, § 3(a) (2018).

151. For a summary of state data protection laws that empower attorneys general, see Serrato et al., *supra* note 125.

152. *See* Charlotte Decker, *Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime*, 81 S. CAL. L. REV. 959, 1010 (noting the methods and difficulty of prosecuting cyber crime). *See generally* Gregory F. Zoeller, *Duty to Defend and the Rule of Law*, 90 IND. L.J. 513 (2015) (noting the broad prosecutorial discretion of the federal government and states' attorneys general).

153. MASS. GEN. LAWS ch. 93H, § 6 (2018) ("The attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.").

154. *See* Aminpour v. Arbella Mut. Ins., No. 15-P-32, 2016 WL 4162417, at *1, 3 (Mass. App. Ct. Aug. 5, 2016).

155. *See id.* at *3. The court noted the lower court's holding that "on the parties' cross motions for partial summary judgment" the lower court "dismiss[ed] the plaintiff's claim

language of this statute, and subsequent court decisions, individual plaintiffs are precluded from bringing an action under chapter 93H against a negligent data storage provider in Massachusetts, even if the defendant company did, in fact, fail to comply with the statute's safety requirements.[156] Ironically, this statute was enacted to protect Massachusetts consumers from data breaches; however, the consumers themselves cannot seek redress if, in fact, they suffer harm from non-compliance.[157]

c. Other actions by the Massachusetts Attorney General

The apparent lack of an individual cause of action leaves enforcement solely in the hands of the attorney general. In another matter, the Massachusetts Attorney General brought suit against Multi-State Billing Services (MSB), a Medicaid billing company, after a laptop that had more than 2,600 Massachusetts children's unencrypted personal data and information was stolen.[158] The evidence showed that MSB failed "to take reasonable steps to safeguard the personal information from unauthorized access or use."[159]

> [T]he complaint allege[d] that the company failed to develop, implement, and maintain a written and comprehensive information security program, train members of its workforce on how to reasonably safeguard personal information, or maintain a computer security system that ensured that personal information stored on laptop computers or other portable devices was encrypted.[160]

---

under chapter 93H on the ground that there [wa]s no private right of action under this statute." *Id.*

156. *See* Owen Weaver, *A Missed Opportunity to Bolster Consumer Protection in Massachusetts: How Massachusetts Residents Are Still Without a Private Right of Action After the TJX Security Breach*, 43 NEW ENG. L. REV. 677, 704–06 (2009).

157. *See* Katz v. Pershing, LLC, 806 F. Supp. 2d 452, 458 (D. Mass. 2011).

> More fundamentally, the power to enforce Chapter 93H is limited to the State Attorney General—the statute does not incorporate or otherwise authorize a private right of action. The enforcement section of Chapter 93H provides that the "attorney general may bring an action pursuant to . . . chapter 93A against a person or otherwise to remedy violations of this chapter . . . ." Because Katz cannot maintain an action under Chapter 93A based on an alleged violation of Chapter 93H, she cannot look to the state consumer protection statute to establish standing.

Id. (quoting Mass. Gen. Laws ch. 93H §6 (2018)).

158. *See* Press Release, Office of Attorney General Maura Healey, AG Healey Settles with Billing Company over Data Breach Impacting Children (Nov. 29, 2017), https://www.mass.gov/news/ag-healey-settles-with-billing-company-over-data-breach-impacting-children [https://perma.cc/K8SF-ZQK4].

159. *Id.*

160. *Id.*

MSB consented to paying $100,000 and agreed to implement improved security practices after it was "found [to have] violated state consumer protection and data security laws."[161]

III. RECOMMENDATIONS FOR IMPROVING DATA SECURITY BY STRENGTHENING CONSUMERS' ABILITY TO SUE

A. *Leveraging and Expanding Existing State Consumer Protection Laws*

Massachusetts provides some of the most comprehensive consumer protection laws in the country. Specifically, chapter 93A, section 9 of the Massachusetts General Laws states that:

> Any person . . . who has been injured by another person's use or employment of any method, act or practice declared to be unlawful by section two . . . may bring an action in the superior court, or in the housing court as provided in section three of chapter one hundred and eighty-five C whether by way of original complaint, counterclaim, cross-claim or third party action, for damages and such equitable relief, including an injunction, as the court deems to be necessary and proper.[162]

The broad language of chapter 93A, section 9 does not appear to limit the ability of a data breach victim to file a claim against the data holder. Section 2 goes on to allow claims for consumers who have suffered "methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."[163] And although the FTC does not allow individuals to file claims,[164] the Massachusetts legislature specifically stated that in interpreting section 2, "the courts will be guided by the interpretations given by the Federal Trade Commission and the Federal Courts to section 5(a)(1) of the Federal Trade Commission Act, as from time to time amended."[165] The benefit of this language in section 2 allows individuals to bring claims for unfair and deceptive acts while utilizing the broad FTC interpretations to adjudicate the validity of the causes of action brought under chapter 93A. To determine if, in fact, a private cause of action may exist for victims of data breach first requires an evaluation as to whether being the victim of a data breach constitutes

161. *Id.*
162. MASS. GEN. LAWS ch. 93A, § 9 (2018).
163. *Id.* § 2(a).
164. *See supra* Section II.A.
165. § 2(b) (citation omitted).

an unfair and deceptive act.[166] Due to the fact that using personal data for commercial purposes provides a tremendous value to the online merchant, the merchant should be held to have an obligation to safely and effectively use, store, transmit, and destroy all data collected.

The public would best be served if the merchant's standard of care was based not on simple negligence, but rather on a heightened reasonableness standard that compares the data holder's data protection practices to best practices in the data storage industry. If an individual is able to make out a prima facie case that a Massachusetts entity did not adequately store personal data due to a failure to adhere to industry standards, it should be deemed an unfair and deceptive practice for purposes of chapter 93A. Although it may be argued that any Massachusetts claims regarding data storage and breach must be evaluated using chapter 93H (and thus, can only be brought by the attorney general), nothing in chapter 93H indicates it preempts chapter 93A.[167] An individual bringing the data breach action purely as a chapter 93A claim satisfies both the section 2 definition[168] to justify a cause of action and eliminates the attorney general limitation if the claim were brought subject to chapter 93H. The purpose and legislative history of chapter 93A demonstrate its intended broad scope, and nothing in the text indicates that the statute would limit data breach causes of action.[169] Chapter 93H, on the other hand, relates to the creation of regulations for data protection to protect consumers collectively, and enforcement when these regulations are not followed. In contrast, chapter 93A is broader in context, and allows for claims of unfair and deceptive acts, even if an unfair and deceptive act of data theft does not relate to violations of any regulations.

In addition, it might be possible to argue that individual data breach claims might be cognizable under chapter 93H, despite the limiting

166. In Massachusetts, it is well-established that in order "[t]o determine whether a particular practice is unfair, courts examine [w]hether the practice . . . is within at least the penumbra of some common-law, statutory or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes substantial injury to consumers . . . ." Malden Transp., Inc. v. Uber Tech., Inc., 286 F. Supp. 3d 264, 273 (D. Mass. 2017) (quoting Mass. Eye & Ear Infirmary v. QLT Phototherapeutics, Inc., 552 F.3d 47, 69 (1st Cir. 2009).

167. *See* MASS. GEN. LAWS ch. 93H (2018).

168. "Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." MASS. GEN. LAWS ch. 93A, § 2(a) (2018).

169. *See* Auto Flat Car Crushers, Inc. v. Hanover Ins. Co., 17 N.E.3d 1066, 1076 (Mass. 2014). "[Chapter 93A] 'is a statute of broad impact which creates new substantive rights and provides new procedural devices for the enforcement of those rights.' Recovery under the statute is not 'limited by traditional tort and contract law requirements.'" *Id.* (citation omitted) (quoting Slaney v. Westwood Auto, Inc., 322 N.E.2d 768, 772–73 (Mass. 1975)).

language that grants the attorney general the power to bring claims. Note that the language granting the attorney general the power to pursue claims is not exclusive. As discussed previously, Chapter 93H exclusively limits the ability to pursue recourse under Chapter 93A with the attorney general.[170] However, nothing in the statute states that the right to bring an action is exclusive to the attorney general. If the legislature had intended that the attorney general be the *only* entity able to pursue enforcement under the statute, the language could have been drafted in a manner that said: *the attorney general is the exclusive entity that may bring an action*. The current language certainly permits the attorney general to bring an action but does not expressly limit the ability of private individuals to do so.[171]

B. *Common Law Remedies—Fraud, Negligent Infliction of Emotional Distress, and Breach of Contract*

At common law, fraud generally refers to "an act, omission, or concealment in breach of a legal duty, trust, or confidence justly imposed, when the breach causes injury to another or the taking of an undue and unconscientious advantage."[172] Some courts may find this cause of action can be used by individuals to combat data theft.[173] Specifically, entrusting personal data to a third party for purposes of completing a financial transaction creates both a legal and equitable duty by the data holder to keep the data reasonably secure and out of the hands of unintended third parties.[174] In particular, fraud often arises when the data holder engages

---

170. *See* MASS. GEN. LAWS ch. 93H, § 6 (2018).

171. *See* Piscitelli v. Classic Residence by Hyatt, 973 A.2d 948, 967 (N.J. Super. Ct. App. Div. 2009) ("'The express provision of one method of enforcing a substantive rule suggests that Congress intended to preclude others.' . . . [T]herefore, there is clearly no express private right of action and, after reviewing the appropriate factors, there is no implied private right of action based on a violation of [federal law]." (quoting Alexander v. Sandoval, 532 U.S. 275, 290 (2001))).

172. Vela v. Marywood, 17 S.W.3d 750, 760 (Tex. Ct. App. 2000).

173. *See, e.g.*, Hammond v. Bank of N.Y. Mellon Corp., No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *12 (S.D.N.Y. June 25, 2010). "State consumer protection laws typically are intended to 'identify consumer-oriented misconduct which is deceptive and materially misleading to a reasonable consumer, and which causes actual damages.' Such laws typically allow individuals to bring a cause of action for consumer fraud or unfair competition." *Id.* (citation omitted) (quoting Wilner v. Allstate Ins. Co., 893 N.Y.S.2d 208, 214 (N.Y. App. Div.2010)).

174. *See* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 390 (6th Cir. Sept. 12, 2016).

> Here, Plaintiffs sufficiently allege that their injuries are fairly traceable to Nationwide's conduct. For example, Plaintiffs allege that Defendants failed "to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and other Class Members' [data] to protect against anticipated threats to the security or integrity

in an act or omission that exposes the data to an unauthorized third party. Following the conveyance of personal data, the consumer's data rests in the hands of the data holder, and thus its security and protection is solely entrusted to the data holder. As the consumer trusts the data holder to protect its data, and the data holder has agreed to hold the data safely and securely, failing to take adequate precautions and otherwise allowing the data to be accessed by unauthorized third parties is a breach of that trust and can also constitute negligence.[175]

To succeed on a negligent infliction of emotional distress claim in Massachusetts, the following evidence must be satisfied: "(1) negligence; (2) emotional distress; (3) causation; (4) physical harm manifested by objective symptomatology; and (5) that a reasonable person would have suffered emotional distress under the circumstances of the case."[176] Although challenging, a data theft victim might be successful in pursuing a claim for intentional infliction of emotional distress if the victim is able to demonstrate that the theft has manifested itself in a physical harm with objective symptomatology.[177] As noted in *Sullivan v. Boston Gas Co.*, "[a] successful negligent infliction of emotional distress claim . . . must do more than allege 'mere upset, dismay, humiliation, grief and anger.'"[178] Accordingly, in order for a plaintiff to be successful in a negligent infliction of emotional distress action, in addition to demonstrating that

---

> of such information." Although hackers are the direct cause of Plaintiffs' injuries, the hackers were able to access Plaintiffs' data only because Nationwide allegedly failed to secure the sensitive personal information entrusted to its custody. In other words, but for Nationwide's allegedly lax security, the hackers would not have been able to steal Plaintiffs' data.

Id. (alteration in original) (citation omitted).

175. *See generally* Anthony E. White, *The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who is Going to Pay for It?*, 88 MARQ. L. REV. 847 (2005).

176. Payton v. Abbott Labs, 437 N.E.2d 171, 181 (Mass. 1982).

177. *Szanto v. Szanto*, No. G039194, 2008 WL 4726452, at *7 (Cal. Ct. App., Oct. 29, 2008).

> In short, what Phillip alleged, under the label of "identity theft," was simply an amalgam of a claim for conversion and intentional infliction of emotional distress: i.e., defendant utilized Phillip's personal identity for his own purposes, without Phillip's knowledge or permission (in other words, that he stole it); that he made use of that information in a manner which was "despicable and should not be tolerated in a civil society"; and that the conduct caused both economic damages and serious emotional distress to Phillip. Those allegations were sufficient to survive demurrer, and the court erred in concluding otherwise simply because the allegations had been lumped together under the new label of identity theft.

Id.

178. Sullivan v. Bos. Gas Co., 605 N.E.2d 805, 809–10 (Mass. 1993) (quoting Corso v. Merrill, 406 A.2d 300, 304 (N.H. 1979)).

the data holder acted negligently, the victim must have suffered a physical manifestation that can be diagnosed and introduced in court.

C. *Expanding FTC to Include a Private Cause of Action*

The FTCA requires heightened data protection and provides enhanced protection for consumers but lacks any private enforcement.[179] A congressional adjustment to the FTCA creating a private cause of action for data breach violations will encourage data holders to better comply with the regulations in order to avoid widespread exposure. The FTCA does a tremendous job of regulating data holders; however, enforcement is sparse based on the limited resources of the FTC, and thus only the largest and most high-profile breachers are pursued. By removing the FTCA language that limits enforcement, it is hypothesized that individuals injured by a data breach would be able to seek enforcement, further incentivizing businesses to be exceptionally careful and compliant.

D. *Creating a New Federal Data Security Law Akin to GDPR*

In the alternative to amending the FTCA to allow for a private cause of action, Congress could also look to enact a comprehensive overhaul of the data privacy law by enacting the EU General Data Protection Regulation.[180] GDPR provides wide protections for data usage and storage and also permits private causes of action.[181] Many international companies have already invested the time, money and effort to change their practices to comply with this law, hence extending this protection to their U.S. operations will cause much less effort.

CONCLUSION

Due to the limited risk of prosecution, the profitability of data theft will continue to propel its prevalence. Accordingly, those entrusted with our data need to be vigilant in protecting and combating the increasing levels of complexity used by data thieves. To ensure our data is adequately protected, individuals need to have the right to bring suit to hold the data keeper liable. In turn, the potential liability will force the data holder to maintain a high level of data security, better protecting all consumers and encouraging the continued growth of online commerce. By expanding rights under the FTCA to include a private cause of action, leveraging existing state and common law expansively, and creating

179. *See supra* Section II.A.

180. *See generally* STEPHEN P. MULLIGAN ET AL., CONG. RESEARCH SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW (2019), https://crsreports.congress.gov/product/pdf/R/R45631 [https://perma.cc/7QFT-DDRS].

181. *Supra* Section II.B.1.

comprehensive new federal legislation that mimics the GDPR, consumers will be empowered to hold wrongdoers accountable and in turn, encourage data holders to maximize data security and protection.