2016

Small Companies, Big Breaches: Why Current Data Protection Laws Fail American Consumers in Cases of Third-Party Hacking

Kaylie Gioioso

Kaylie Gioioso*

Small Companies, Big Breaches: Why Current Data Protection Laws Fail American Consumers in Cases of Third-Party Hacking

The number of data breaches resulting in stolen consumer identities continues to soar in the United States as businesses increase their online presences.[1] Small businesses have been particularly and disproportionately impacted.[2] Hackers are increasingly attacking smaller vendors with weak security systems as entry points into the systems of large corporations, a phenomenon known as third-party hacking.[3] Current laws, which require only that reasonable security measures *in light of a company's size*, offer little consumer protection from these third-party breaches.[4] Lawmakers could better serve American consumers by deferring to state law regimes. Individual states should pass laws that focus on comprehensive data security and give states' attorney generals broad enforcement power.[5] Part I of this comment discusses the general background surrounding data breaches, part II discusses the current legal landscape, part III analyzes the efficacy of the reasonableness standard, and finally, part IV suggests ways in which data breach laws can be improved upon moving forward.

* J.D., University of Maryland Francis King Carey School of Law, 2016; B.B.A. in Economics, *summa cum laude*, Loyola University Maryland, 2012. I would like to thank the members of the Journal of Business & Technology Law for their very helpful feedback in writing this comment. I dedicate this comment to my parents, Holly and Wayne Gioioso, Jr., and my siblings, Kara, Lily, and Bennett, for all of their love and support. I also dedicate this comment to Alex Stern for making law school the best three years of my life!

1. *See infra* Section I.A.
2. *See infra* Section I.B.
3. *See infra* Section I.D.
4. *See infra* Section II.A.
5. *See infra* Section IV.

I. Background

A typical day in the life of an American consumer is increasingly conducted online. Grocery orders, retail purchases, entertainment consumption, employment searches, and even romantic interactions are just a few of the many ways in which consumers transact online. The convenience that accompanies these online services necessarily translates into the online sharing of personal information with the companies that facilitate the transactions, which in turn results in the increased theft of personal information through data breaches.[6] A data breach is defined as "an incident in which an individual name plus a Social Security number, driver's license number, medical record, or financial record" is put at risk.[7]

A. Data breaches are an increasingly pressing threat to American consumers' privacy.

Data breaches present a bigger threat to American consumers' privacy than ever before. Robert Mueller, former director of the Federal Bureau of Investigation, recently warned that "there are only two types of companies: those that have been hacked and those that will be."[8] A staggering number of U.S. companies have been the victims of data breaches, resulting in the theft of millions of consumers' personal data.[9] For example, since 2005, approximately 675 million personal records have been exposed due to data breaches.[10] In 2014, the number of U.S. data breaches reached an all-time high of 783 reported incidents,[11] representing a 27.5% increase since 2013.[12] Although not all data breaches result in identity theft,[13] criminal attacks (as opposed to system glitches or negligence) are by far the most frequent causes of data breaches, representing 44% of all reported incidents.[14]

As the sheer number of attacks has increased, so has the cost for both the individual companies and consumers. For companies, from 2013 to 2014, the

6. *How the Desire for Increased Convenience is Having an Impact on Privacy*, McCuneWright, LLP, (Dec. 14, 2015), http://mccunewright.com/how-the-desire-for-increased-convenience-is-having-an-impact-on-privacy/.

7. *Data Breaches*, Identity Theft Res. Ctr., http://www.idtheftcenter.org/id-theft/data-breaches.html. (last visited Feb. 23, 2016).

8. Douglas H. Meal, *Private Data Security Breach Litigation in the U.S.*, Aspatore 1, 1 (2014), https://www.ropesgray.com/~/media/Files/articles/2014/February/Meal%20Chapter.ahx.

9. *See Identity Theft Resource Center Breach Report Hits Record High in 2014*, Identity Theft Res. Ctr., (Jan. 12, 2015), http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html.

10. *Id.*

11. *Id.* (noting that this number is a safe estimate, as many data breaches "fly under the radar" and go unreported).

12. *Id.*

13. *Id.*

14. *2014 Cost of Data Breach Study: U.S.*, Ponemon Inst. Research Report 1, 9 (May 2014) http://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf. System glitches represent 25 percent of data breaches while negligence represents 31 percent of data breaches. *Id.*

average cost of an organizational data breach increased from $5.4 million to $5.9 million.[15] The cost per individual record[16] stolen per breach increased from $188 to $201.[17] The average cost of lost business due to a breach increased by 15% to $3.5 million.[18] In total, data breaches cost the American economy approximately one billion dollars annually.[19]

For individuals, the cost of having their personal information compromised varies depending on what information is stolen, and how quickly the theft is discovered.[20] Financial costs can range anywhere from $50 to several thousand dollars,[21] but the emotional harms suffered can be far costlier.[22] In a survey by the Identity Theft Resource Center, victims of identity theft reported feeling vulnerable, helpless, betrayed, and embarrassed, in addition to losing sleep and their general peace of mind.[23] Victims described having their credit history destroyed and having to pay much higher interest rates on any new credit cards, as well as spending countless hours trying to undo the damage caused by the hackers.[24]

While multimillion-dollar companies suffer the highest dollar losses, and individuals suffer the greatest emotional harm, a third category of entities affected by data breaches is often overlooked.[25]

B. Data breaches have a significant negative impact on small businesses.

As the number of data breaches has continued to increase, perhaps no group has been more severely impacted than small businesses.[26] Cybersecurity firm Symantec has reported significant increases in cyberattacks on small businesses over the past

15. *Id.* at 6.

16. A record is any personal information associated with one person. *Id.* at 3.

17. *Id.* at 5.

18. *Id.* at 1.

19. Steve Viuker, *Cybercrime and Hacking are Even Bigger Worries for Small Business Owners*, THE GUARDIAN (Jan. 21, 2015, 3:18 P.M.), http://www.theguardian.com/business/2015/jan/21/cybersecurity-small-business-thwarting-hackers-obama-cameron.

20. Kimberly Rotter, *The Staggering Costs of Identity Theft in the U.S.*, CREDIT SESAME (Jun. 19, 2014), http://www.creditsesame.com/blog/staggering-costs-of-identity-theft/.

21. *Id.*

22. *See* Herb Weisbaum, *ID Theft Can Take Heavy Emotional Toll on Victims*, TODAY (Nov. 20, 2014, 12:11 P.M.), http://www.today.com/money/id-theft-can-take-heavy-emotional-toll-victims-1D80305639.

23. *Id.*

24. *Id.*

25. *Infra* Section I.B.

26. Parija Kavilanz, *Cybercrime's Easiest Prey: Small Businesses,* CNN MONEY (Apr. 23, 2013, 4:00 p.m.), http://money.cnn.com/2013/04/22/smallbusiness/small-business-cybercrime/. According the Small Business Association, the definition of a small business depends on the industry in which the company operates. *Table of Small Business Size Standards*, U.S. SMALL BUSINESS ASSOCIATION https://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf, (last visited Dec. 2, 2015). However, a small business consists of no more than 500 employees and an average annual receipt of less than 15 million dollars. *See id.*

several years,[27] with the number of attacks on these companies increasing 300% from 2011 to 2012.[28] Similarly, the National Cyber Security Alliance recently reported that out of over one billion attempted cyberattacks prevented by Symantec in 2012,[29] almost 40% specifically targeted small businesses.[30] Additionally, one in five small businesses is a victim of a cyberattack every year.[31] Even more worrisome is the fact that about 60% of these companies go out of business within six months after being hacked,[32] as each breach costs small businesses thousands of dollars on average,[33] a hit many of the companies cannot survive.[34]

The stories surrounding these attacks on small companies all sound eerily similar. For example, take the story of the cyber attack on specialty T-Shirt company 80sTees.[35] A credit card company notified the owner of the store that some customers were complaining of mystery charges.[36] 80sTees promptly ceased collecting customers' credit card information, had the matter investigated by its own expert and reported the incident to the federal government.[37] However, the investigation yielded no evidence of an intrusion to the system, and 80sTees continued business as usual.[38] Flash forward several months and credit card complaints later, and the company's fears were confirmed.[39] Their system had in fact been hacked at the time of the original complaint, and thousands of customers' data was stolen.[40] The company was forced to stop collecting credit card data from customers for four months while it developed a new website and implemented new internal safety measures, suffering major revenue losses along the way. [41]

---

27. *Small Firms Cybersecurity Guidance*, SIFMA 1, 3 (July 2014), https://www.sifma.org/WorkArea/DownloadAsset.aspx?id=8589949972.

28. John Brandon, *Why Your Business Might be a Perfect Target for Hackers,* INC. (Jan. 2014), http://www.inc.com/magazine/201312/john-brandon/hackers-target-small-business.html.

29. *New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity*, NAT'L CYBER SEC. ALL., https://staysafeonline.org/about-us/news/new-survey-shows-us-small-business-owners-not-concerned-about-cybersecurity, (last visited Feb. 23, 2016).

30. *Id.*

31. Robert Strohmeyer, *Hackers Put a Bull's-Eye on Small Business,* PCWORLD (Aug. 12, 2013, 3:30 AM), http://www.pcworld.com/article/2046300/hackers-put-a-bulls-eye-on-small-business.html.

32. *Id.*

33. E. Scott Reckard & Tiffany Hsu, *Small Business at High Risk for Data Breach,* LA TIMES (July 4, 2014, 5:07 PM), http://www.latimes.com/business/la-fi-small-data-breaches-20140705-story.html#page=1.

34. *Id.*

35. Jonathon Berr, *A Fast-Growing Threat to Small Businesses: Hackers,* CNBC (Sept. 8, 2014, 10:33 AM), http://www.cnbc.com/id/101971980.

36. *Id.*

37. *Id.*

38. *Id.*

39. *Id.*

40. *Id.; see also* Reckard, *supra* note 33.

41. *See* Reckard, *supra* note 33.

A California-based small business, Rosenthal Wine Bar and Patio, suffered a similar fate when it discovered malware[42] on its computer systems and was unable to identify how long the hackers had been collecting its customers' data.[43] After properly notifying its consumers, "the reaction was immediate."[44] Many customers cancelled their memberships and the company received scathing reviews on Yelp.[45] The company felt as though it had lost much of the good will it had worked so hard to establish in its community.[46] These effects are often fatal to small businesses, resulting in over half of the victim companies going out of business less than a year after an attack.[47]

C. Small businesses have many characteristics that render them particularly attractive to hackers.

Most small businesses have common characteristics that leave them particularly exposed to the threat of cyberattacks and attractive to hackers.[48] First, small businesses often have relatively weak security measures in place.[49] Small businesses typically "lack an IT department and tend not to be as diligent as larger companies about security."[50] Additionally, small companies are doing more and more business "via cloud services that don't use strong encryption technology."[51] Finally, owners of small businesses may lack the funds or the time to invest in more stringent security measures.[52]

Small businesses are also vulnerable because they "don't know what they don't know."[53] In other words, they are unaware of what cyberattacks look like or what types of online activities are risky.[54] For example, a "perfectly normal-looking e-mail from a friend's computer that was attacked without the owner's knowledge could lead to trouble."[55] Similarly, many owners of small businesses falsely believe that

42. Malware is defined as "software programs designed to damage or do other unwanted actions on a computer system." *Malware Definition,* TECH TERMS, http://techterms.com/definition/malware (last visited Feb. 25, 2016).

43. Reckard, *supra* note 33.

44. *Id.*

45. *Id.*

46. *Id.*

47. Graham Winfrey, *Can Your Company Survive a Cyber Attack?,* INC. (Dec. 5, 2014), http://www.inc.com/graham-winfrey/how-to-protect-your-company-information-in-the-digital-age.html.

48. Brandon, *supra* note 28.

49. Berr, *supra* note 35.

50. *Id.*

51. Brandon, *supra* note 28.

52. Associated Press, *Hacking a Big Danger for Small Business,* SF GATE (Oct. 11, 2014, 8:09 PM), http://www.sfgate.com/business/article/Hacking-a-big-danger-for-small-businesses-5817263.php.

53. *Id.*

54. *Id.*

55. *Id.*

they would never be the targets of an attack because they do not collect nearly as much data as the Fortune-500 firms, and therefore fail to adequately protect themselves.[56] The weaker security systems that result from the combination of these factors "translate into reams of sensitive data behind a door with an easy lock to pick" for experienced hackers.[57]

D. Hackers are using small business hacks as entry points for hacking larger corporations.

The relatively weak security systems of small businesses present opportunistic hackers with a way to access the systems and data of larger companies,[58] an occurrence referred to as collateral, or third-party, hacking.[59] The exact mechanisms used by hackers vary, but the general idea is as follows. First, a hacker gains access to a weakly protected online system of a small business.[60] Second, the hacker uses this access as an entry point to a larger company that is connected in some way to the small firm,[61] often as a supplier or contracting party.[62] A perfect example of this phenomenon is the widely publicized data breach of major retailer Target in 2013.[63] Hackers first infiltrated a heating, ventilation, and air conditioning company that had contracted with Target, used "that access to gain a foothold on an internal system and then use[d] that to leapfrog to other systems inside Target's network."[64] Similarly, millions of Home Depot customers had their data stolen when hackers accessed the improvement store's network by using a vendor's stolen log-on credentials in order to "install custom-built malware that stole customer payment-card data and e-mail addresses."[65]

56. Geoffrey A. Fowler & Ben Worthen, *Hackers Shift Attacks to Small Firms,* Wall St. J. (Jul. 21, 2011).

57. Brandon, *supra* note 26.

58. Fowler, *supra* note 56.

59. Collateral hacking is "when a company's critical data is compromised as a result of a third party in possession of the company's sensitive data being hacked. Rather than directly hacking into a company, collateral hackers go through a third party in order to get to the company's sensitive data." *What is the Definitition of Collateral Hacking,* Glob. Mkt., http://wiki.globalmarket.com/what-is-the-definition-of-collateral-hacking-24691.html (last visited Feb. 25, 2016).

60. *See* Jaikumar Vijaya, *Hackers Hit More Businesses Through Remote Access Accounts,* ComputerWorld, (Jul. 2, 2014, 8:48 AM), http://www.computerworld.com/article/2491431/security0/hackers-hit-more-businesses-through-remote-access-accounts.html (describing how hackers recently gained access to several U.S. restaurants through third-party vendors.).

61. Brandon, *supra* note 28 ("If [a small business has] any Fortune 500 companies as customers, you're an even more enticing target—you're an entry point.").

62. *See* Vijaya, *supra* note 60.

63. *Id.*

64. *Id.*

65. Michael Winter, *Home Depot Hackers Used Vendor Log-On to Steal Data, E-mails,* USA Today, (Nov. 7, 2014, 8:57 AM), http://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/.

Reports of third-party attacks like these are becoming more and more common.[66] Furthermore, these third-party hacks occur against the background of a legal framework that is largely failing to protect American consumers, as discussed in Sections III and IV.[67]

II. Legal Background

Federal laws primarily focus on the reasonableness of a company's data security plan in light of that company's size. Additionally, federal laws remain primarily focused on highly regulated industries, like finance and healthcare. The Federal Trade Commission retains the power to regulate consumer-based industries, but has largely refrained from doing so. State laws similarly focus on the reasonableness of a company's data protection plan.

A. Federal laws are largely focused on highly regulated industries and the reasonableness of a company's data protection plans.

The federal government currently enforces a handful of laws related to data security.[68] These laws do not concern most private corporations,[69] but rather address data breaches almost exclusively in: (i) discreet, highly regulated industries, like financial services, consumer reporting, or healthcare,[70] or (ii) specific government agencies, like the U.S. Department of Veterans Affairs.[71] For breaches in the private sector, the few applicable federal laws focus primarily on the reasonableness of the company's security system.[72]

i. Federal laws on cyber security focus primarily on large companies in highly regulated industries.

The most prominent federal data breach laws focus on specific, highly regulated industries.[73] The Financial Services Modernization Act, commonly referred to as the Gramm-Leach-Billey Act,[74] regulates the financial services industry's collection of

66. Vijaya, *supra* note 60.

67. *See infra* Sections III–IV.

68. Jessica Rich, *Data Security: Why It's Important, What the FTC is Doing About It* (Mar. 24, 2014), 2014 WL 1309704 1, 2 (F.T.C.).

69. State laws generally regulate private corporations. *See infra* Section II.B.

70. Rich, *supra* note 68, at 3.

71. *See* 38 U.S.C. § 5723 (2012).

72. *See infra* Section II.A.iii.

73. Rich, *supra* note 68, at 3.

74. 15 U.S.C. § 6801 (2012).

consumer data.[75] Gramm-Leach-Billey requires financial institutions to "develop procedures for protecting the security of customer data" and empowers several government agencies to enforce the relevant regulations.[76] One section of the Gramm-Leach-Billey Act, referred to as the Safeguards Rule, imposes regulations on non-bank financial institutions, and allows the FTC to take law-enforcement action against companies that are not in compliance with the data security requirements.[77]

Similarly, federal laws regulate data collection in the credit-reporting and healthcare industries.[78] The Fair Credit Reporting Act mandates that credit-reporting agencies only disclose private consumer information to entities which have a "permissible purpose" for requesting data, and additionally "imposes safe disposal obligations" on companies that receive such data.[79] The healthcare and health insurance industries are regulated by the Health Insurance Portability and Accounting Act, which aims to protect consumer privacy by establishing nationwide security and use standards for institutions that collect individual medical records and personal health information.[80]

ii. Federal laws also regulate cyber security for government agencies.

The federal government has also enacted data breach laws in its own agencies.[81] The Federal Information Security Management Act (FISMA) "establishes a framework designed to ensure the effectiveness of security controls over information resources that support federal operations and assets."[82] Agencies including the Department of Veterans Affairs,[83] and the Department of Education are responsible for developing and implementing their own security and risk management procedures.[84] The

75. Office of the Attorney Gen., *Financial Privacy: The Gramm-Leach Bliley Act*, State of Idaho, http://www.ag.idaho.gov/consumerProtection/generalTopics/topicSubPages/financialPrivacy.html (last visited Dec. 2, 2015).

76. Paul M. Schwartz, *Notification of Data Security Breaches*, 105 Mich. L. Rev. 913, 920 (2007).

77. Rich, *supra* note, 68 at 3.

78. *Id.*

79. *Id.*

80. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (Aug. 21, 1996).

81. *Information Security: Federal Agencies Need to Enhance Responses to Data Breaches: Testimony Before the Comm. On Homeland Sec. and Govt. Affairs,* U.S. Sen. 1, 5 (Apr. 2, 2014) (testimony of Gregory C. Wilshusen, Director of Information Security Issues), http://gao.gov/assets/670/662227.pdf.

82. *Id.;* Federal Information Security Management Act of 2002, H.R. §§ 3541–3549 (2002).

83. *See supra* Section II.A.

84. Wilshusen, *supra* note 81, at 7 (stating that the 24 major agencies that have partially or fully implemented data security procedures are as follows: "the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.").

Federal Trade Commission oversees the implementation of FISMA, but the individual agencies are largely left to their own discretion in choosing security measures.[85]

iii. The Federal Government has the option to regulate private industry and small companies under the Federal Trade Commission Act of 1914, but has largely chosen not to do so.

Lastly, the FTC has the power to regulate the collection of personal information by national retail corporations outside of the highly regulated financial and healthcare industries.[86] The FTC enforces laws regarding consumer data security under Section 5 of the Federal Trade Commission Act of 1914.[87] However, the protection that this law offers is limited in scope, as it only enables the FTC to act in cases of unfair or deceptive practices by a company in relation to its data security measures.[88]

In a recent statement, the Director of the Bureau of Consumer Protection for the FTC, Jessica Rich, described the FTC's general approach toward data security.[89] She explained that:

> *The touchstone of the FTC's approach to data security, under whatever law we are applying, is reasonableness: a company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.*[90]

This approach allows for the consideration of several factors, including: whether the risk of breach was obvious or foreseeable, the relative costs and benefits of additional security measures, and the current availability of protective tools on the market.[91]

Companies are accordingly only required to take "reasonable" steps to ensure consumer privacy but the FTC does not provide specific, tailored requirements, so "[t]here is more than a fair amount of leeway for entities in deciding what data security measures to take."[92] Under this standard, the FTC has only pursued

85. *Id.* at 5.

86. *See* Rich, *supra* note, 68 at 3–4.

87. *Id.*; 15 U.S.C. § 45 (2012).

88. Rich, *supra* note, 68 at 3–4.

89. *Id.*

90. *Id.* at 4.

91. *Protecting Consumer Info.: Can Data Breaches Be Prevented?: Hearing Before the Comm. On Energy & Commerce & Subcomm. On Commerce, Mfg., & Trade* 1, 4 (Feb. 5, 2014), (statement of Edith Ramirez, Chairwoman of the FTC), http://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-consumer-information-can-data-breaches-be/140205databreaches.pdf.

92. Paul M. Schwartz, *Notification of Data Security Breaches*, 105 Mich. L. Rev. 913, 922 (Mar. 2007).

approximately fifty cases for violations under this law in the thirteen years since 2001.[93] Compared to the thousands of disclosed incidents of data breach during this same time, the FTC's number of actions seems miniscule.[94]

B. The state and local legal environments are similarly aimed at large companies, requiring only reasonable security measures in relation to a company's size.

Consumer information protection laws for retail and non-financial services companies are primarily enacted and enforced on the state level.[95] State statutes, in addition to common law tort principles, govern cases involving data breaches.[96]

California led the nation in enacting data breach legislation when it passed the statute S.B. 1386 in 2003.[97] Many other states went on to enact similar legislation, basing their respective statutes on California's model.[98] California's statute and many of the subsequent statutes modeled after California's largely have one thing in common with the federal data breach laws:[99] the statutes require only "reasonable" security measures in light of a company's size and capabilities.[100]

For example, Maryland's Personal Information Protection Act provides that:

> *a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations.*[101]

The Maryland legislature did not specifically detail what qualifies as "reasonable" for any given size company in the Act, but chose instead to leave this vague

93. Ramirez, *supra* note 91, at 4.

94. Robert D. Brownstone, 1 DATA SEC. & PRIVACY LAW § 9:101 (2014), Chapter 9: Privacy Litigation.

95. Schwartz, *supra* note 92 at 915. Forty-six states, plus the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, have enacted data breach notification legislation. The only four states that have not enacted such legislation are Alabama, Kentucky, New Mexico, and South Dakota. Brownstone, *supra* note 94.

96. Schwartz, *supra* note 99 at 923.

97. *Id.* at 915; CAL. CIV. CODE § § 1798.29, .82, .84 (West 2006).

98. Schwartz, *supra* note 92 at 915.

99. *Supra* Section II.A.

100. For example, California's statute provides that: "A business that owns or licenses personal information about a California resident shall implement and maintain *reasonable* security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." CAL. CIV. CODE § § 1798.81.5(b) (West 2006) (emphasis added). Maryland's statute adds the requirement that the security procedures be reasonable in light of the "nature and size of the business and its operations." MD CODE ANN., COM. LAW, § 14-3503(a) (West 2013).

101. MD CODE ANN., COM. LAW, § 14-3503(a) (West 2013). Other states with a reasonable requirement include Arkansas, California, Nevada, Oregon, Rhode Island, Tennessee, Utah, and Washington. *See* Mintz Levin, LLC, *State Data Security Breach Notification Laws,* MINTZ (Jan. 1, 2015), https://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf.

requirement up to interpretation.[102] The logical presumption follows, then, that security measures considered "reasonable" for a small company would not be considered as such for a larger, multi-state corporation. Small companies can legally have "small" security measures in place.

III. Analysis of Data Security Under the Reasonableness Standard

Upon first glance, the reasonableness requirement directed at big companies makes sense. Larger corporations have more consumers, and thus more data, to protect. However, closer inspection reveals that the vague reasonableness standard, without any additional safeguards, is failing American consumers.[103] Hackers gain easier access to small companies' weakly (but still "*reasonably,*" in light of their size) protected systems and use this access as a gateway to the larger companies' databases.[104] The *reasonableness* requirement in both federal and state laws, as currently applied, fails to protect America's consumers from having their personal information stolen.[105]

A *reasonable* data protection plan for a small business might look something like the following: first, the company should train its employees in basic data security practices, like strong passwords and Internet use guidelines.[106] Second, the company may install basic antivirus software[107] and scan the software after any updates to detect any new viruses,[108] as well as provide a basic firewall[109] for Internet connections.[110] Finally, the small company may control physical access to computers, limit employee access to customer information files, and make backup copies of important data.[111] Again, none of these security measures are specified or currently required by law,[112] but instead constitute what would likely be considered a *reasonable* system under federal and state data protection laws.[113]

---

102. MD Code Ann., Com. Law, § 14-3503(a) (West 2013).

103. *See generally* Michael Winter, *Home Depot Hackers Used Vendor Log-On to Steal Data, E-mails,* USA Today (Nov. 7, 2014, 8:57 AM), http://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/.

104. *Id.*

105. *Infra* Section III.

106. *Cybersecurity for Small Businesses,* Fed. Commc'n Comm'n, http://www.fcc.gov/cyberforsmallbiz (last visited Dec. 2, 2015).

107. *Id.*

108. *Id.*

109. A firewall is defined as "the primary method for keeping a computer secure from intruders. A firewall allows or blocks traffic into and out of a private network or the user's computer." Definition of Firewall, PC Mag, http://www.pcmag.com/encyclopedia/term/43218/firewall (last visited Dec. 2, 2015).

110. Cybersecurity for Small Businesses, *supra* note 106.

111. *Id.*

112. *Supra* Section II.A–B.

113. Cybersecurity for Small Businesses, *supra* note 106.

On the other hand, a standard, reasonable data protection plan for a large corporation is predictably far more complex.[114] A reasonable "big data" [115] plan might involve additional precautions that supplement the protective measures described above.[116] First, the company should implement an organization-wide, in-depth security strategy for dealing with suspected and confirmed breaches.[117] This includes logging every "access and manipulation of" data by all employees;[118] the log must then be "audited regularly (on a weekly or less period), and ideally the logs should be automatically monitored by anomaly detection systems for inappropriate usage and unexpected patterns."[119] Second, the company should install automatic scanning systems that constantly monitor[120] the network for vulnerabilities.[121] Third, big data companies should encrypt[122] individual data records stored in their networks.[123] Finally, companies may wish to establish a hotline to provide company personnel with immediate access to pre-approved data breach attorneys, experts, and/or an information technology support team so that suspicious activities can immediately be reported and evaluated in order to determine the level of response it warrants.[124] These additional precautions likely constitute a reasonable security system for a big data company.

Under the applicable federal and state laws,[125] both security systems described above would likely be considered reasonable by state courts or the FTC.[126] The hypothetical small business presumably has fewer resources and a lower volume of

114. Jeff Markey, *How to Manage Big Data's Big Security Challenges,* Data Informed (May 13, 2014), http://data-informed.com/manage-big-datas-big-security-challenges/.

115. Classification of sets of data as big data is based on the volume, velocity, and variety of data collected. *Big Data: What It Is and Why it Matters*, SAS: The Power to Know, http://www.sas.com/en_us/insights/big-data/what-is-big-data.html (last visited Dec. 2, 2015).

116. *Supra* notes 106–111.

117. Nate Lord, *Enterprise Security Breaches: Data Security Experts on How an Enterprise can Protect Itself from a Big Data Security Breach*, Digital Guardian (Jan. 7, 2015), https://digitalguardian.com/blog/enterprise-security-breaches-data-security-experts-how-enterprise-can-protect-itself-big-data.

118. *Id.*

119. *Id.*

120. This is in contrast to the virus protection software of small companies, which may only scan at set intervals or after updates. *Supra* note 106.

121. Lord, *supra* note 117.

122. Encryption is "the conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties." *Encryption,* TechTarget, http://searchsecurity.techtarget.com/definition/encryption (last visited February 21, 2016).

123. Lord, *supra* note 117.

124. *Id.*

125. *Supra* Section II.A–B.

126. Jessica Rich, *Data Security: Why It's Important, What the FTC is Doing About It,* (Mar. 24, 2014), 2014 WL 1309704 1, 4 (F.T.C.) (describing the FTC's general approach to data security); The Federal Trade Commission Act, 15 U.S.C. § 45 (2012)*; see, e.g.* MD Code Ann., Com. Law, § 14-3503(a) (West 2013).

consumer data,[127] which means it can have a far less sophisticated security system in place and remain in compliance with all relevant laws.[128] The hypothetical "big data" company has more resources and collects more consumer records, so it must maintain a higher-level data protection plan in order to comply with the reasonableness standard under the law.[129]

This discrepancy seems "reasonable" upon first glance, but upon closer examination reveals a glaring loophole which hackers can and have exploited to the detriment of American consumers.[130] Even the most sophisticated of hackers would find it easier and more efficient to attack the weaker security system of the small businesses.[131] This does not present a huge problem initially, as the small business has a relatively small amount of private data that would be compromised.[132] The issue becomes a much larger one, literally and figuratively, if that small business contracts with a big data company and has insider, password-protected access to the larger company's network.[133] The small company acts as a "gateway" to the larger company and allows hackers easier access than if they attacked the big data company from the start.[134] The hack and data breach of big data companies occur because of the lower security requirements for these smaller companies, exposing millions of consumers' personal data that would otherwise be protected, but for these smaller companies' weaker security systems. Injured consumers, however, are left without recourse, because both companies' security systems are in compliance with the law, as they are *reasonable* for their respective sizes.[135]

The reasonableness requirement based on the size of the company, without any additional security requirements, is failing our country's consumers. As noted

127. As compared to the resources of the "big data" corporations. Stuart Wall, *How and Why Data Will Save Small Business,* SMALL BUSINESS TRENDS (Mar. 20, 2015), http://smallbiztrends.com/2015/03/small-business-data-collection.html.

128. The Federal Trade Commission Act, 15 U.S.C. § 45 (2012)*; see, e.g.* MD CODE ANN., COM. LAW, § 14-3503(a) (West 2013).

129. *See* The Federal Trade Commission Act, 15 U.S.C. § 45 (2012).

130. *See* Jaikumar Vijaya, *Hackers Hit More Businesses Through Remote Access Accounts,* COMPUTERWORLD (Jul. 2, 2014) http://www.computerworld.com/article/2491431/security0/hackers-hit-more-businesses-through-remote-access-accounts.html (describing the Target third-party breach); *see also* Michael Winter, *Home Depot Hackers Used Vendor Log-On to Steal Data, E-mails,* USA TODAY (Nov. 7, 2014, http://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/ (describing the Home-Depot third-party breach).

131. Constance Gustke, *No Business Too Small to Be Hacked,* N.Y. TIMES (Jan. 13, 2016), http://www.nytimes.com/2016/01/14/business/smallbusiness/no-business-too-small-to-be-hacked.html?_r=0.

132. Wall, *supra* note 127.

133. Jen A. Miller, *How the Target Breach Has Affected Small Business Data Security,* CIO (Jul. 9, 2014), http://www.cio.com/article/2451283/data-breach/how-the-target-breach-has-affected-small-business-data-security.html (describing how hackers used an HVAC vendor's log-in credentials as a gateway into Target's payment system).

134. *Id.*

135. The Federal Trade Commission Act, 15 U.S.C. § 45 (2012)*; see, e.g.* MD CODE ANN., COM. LAW § 14-3503(a) (West 2013).

earlier, multiple data breaches of huge, household name companies have occurred because hackers gained access to small company contractors first.[136] In the Target breach, hackers infiltrated the retailer by first attacking an HVAC company and using the contractor's credentials to access Target's network.[137] Seventy million customers had their names, addresses, emails, and phone numbers stolen; another forty million also lost credit card numbers.[138] In another massive attack, hackers used a third-party vendor's log-in information to penetrate Home-Depot's network.[139] Fifty-six million Americans' credit card numbers were compromised.[140] Similarly, Goodwill suffered a massive breach when a hacker attacked a third-party credit-card processing vendor and subsequently obtained access to Goodwill customers' credit card information.[141] Debit and credit card information of 868,000 customers was stolen.[142]

Stories like these are becoming more and more frequent, and the applicable laws are becoming less and less adequate. In most incidences of third-party hacking, both companies' security systems are in compliance with the law,[143] but wholly fail to protect consumers. Consumers are left without recourse and the law provides no incentive for companies to make meaningful changes.[144] The time has come for the vague reasonableness standard to be supplemented with stricter, data protective state laws.[145]

IV. Recommended Changes

Many suggestions have been put forth as to how to best handle the growing number of data breaches in this country.[146] These suggestions range from reliance on tort theories of strict liability[147] to legislation requiring companies to implement a strict, standardized set of security measures.[148] One possible solution that has gained

136. *Supra* Section I.D.

137. Miller, *supra* note 133.

138. *Id.*

139. Michael Winter, *Home Depot Hackers Used Vendor Log-On to Steal Data, E-mails,* USA Today (Nov. 7, 2014), http://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/.

140. *Id.*

141. Bill Hardekopf, *The Big Data Breaches of 2014,* Forbes (Jan. 13, 2015), http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/.

142. *Id.*

143. The Federal Trade Commission Act, 15 U.S.C. § 45 (2012)*; see, e.g.* MD Code Ann., Com. Law, § 14-3503(a) (West 2013).

144. *See supra* Sections II.A—B.

145. *See infra* Part IV.

146. *See generally* Danielle Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age,* 80 S. Cal. L. Rev. 241 (2007).

147. *Id.* at 268—277.

148. Natasha Lomas, *Call for Robust Privacy Legislation in Wake of EU Safe Harbor Strike-Down,* TechCrunch (Oct. 28, 2015), http://techcrunch.com/2015/10/28/fundamental-rights-vs-self-regulation/.

ground in recent years is the call for a national federal law that would preempt state data protection laws.[149] This suggestion is misguided, however, as it could undo the strides that several states have taken in passing relatively strict data breach legislation.[150] Instead, Congress should defer to individual states, which should in turn: (1) pass data protection laws that rely on comprehensive best practices approaches; and (2) give states' attorney generals broad enforcement authority.[151] This approach provides companies with more explicit guidelines than a vague reasonableness standard alone, and therefore better protects American consumers from the growing problem of third-party hacking.

A. The call for a national federal data breach law is a misguided suggestion that would ultimately harm American consumers.

Recently, there has been a push for Congress to adopt a nationwide data breach law that would preempt existing state laws.[152] Industry groups argue that mismatched and inconsistent state laws make it difficult for companies to know whether they are complying with the law in any given state at any given time.[153] One industry expert argued that the "myriad of conflicting state laws, as well as the lack of one over-arching federal law, creates legal and compliance nightmares for companies that these breaches affect."[154] Even President Obama recently called for a national standardized data breach law in a speech to the FTC.[155] In his speech, the President referenced the argument that the various state laws cause consumers and companies alike great confusion, and urged business leaders and privacy advocates to push for the passing of a national standardized law.[156]

This suggestion for a federal data breach law is misguided for two reasons. First, the argument that the myriad of state laws confuses companies is simply not true. In our national economy today, most companies conduct business across state borders.[157] In order to avoid confusion associated with compliance with various state data breach laws, companies typically end up complying with the strictest set

149. Jeffrey K. Douglass, et. al., *High Priority: A Federal Data Breach Notification Law,* Morris, Manning & Martin, LLP (Dec. 3, 2014), http://www.mmmlaw.com/media-room/publications/articles/high-priority-a-federal-data-breach-notification-law.

150. Cory Bennett, *State AGs Clash with Congress over Data Breach Laws,* The Hill (Jul. 7, 2015), http://thehill.com/policy/cybersecurity/247118-state-ags-warn-congress-against-preempting-data-breach-laws/.

151. *Infra* Section IV.B.

152. Douglass, *supra* note 149.

153. Bennett, *supra* note 150.

154. Douglass, *supra* note 149.

155. Maria Korolov, *Obama Proposes New 30-day Data Breach Notification Law*, CFO (Jan. 13, 2015) http://www.csoonline.com/article/2868096/data-protection/obama-proposes-new-30-day-data-breach-notification-law.html.

156. *Id.*

157. Sam Hodges, *Four Big Tax Issues and How They Can Affect Your Business,* Corp! (Jan. 14, 2016), https://www.corpmagazine.com/finance/four-big-tax-issues-can-affect-business/.

of state laws.[158] This way, they are likely also compliant with the less strict state laws, and are able to avoid potential confusion across state lines.[159] A federal law would likely not rise to the level of the strictest state laws, and therefore could very likely represent a step backward in protecting American consumers.[160]

The call for a federal data protection law is also misguided due to the ever-changing nature of technology. Technological advances related to data security occur so quickly that a federal law with standardized protection requirements could become obsolete in a matter of months, if not sooner.[161] Congress is ill-suited to quickly respond to these changes. States and their attorney generals, on the other hand, are often better suited to adopt legislation that is tailored to the changing technological landscape more effectively.[162]

B. The approach best suited to protect American consumers' data is a state law regime that takes a comprehensive approach to data security and gives states' attorney generals broad enforcement power.

Federal lawmakers should forego a national data breach law and instead defer to state laws, which should in turn implement a comprehensive approach to data security that give states' attorney generals broad enforcement powers. In comparison to federal lawmakers, state legislatures are better equipped to quickly adapt to changing technological climates. This would reduce the likelihood that laws would become and remain obsolete.

i. Comprehensive Approach to Data Security

A key factor in a state law regime that could reduce the likelihood of obsolescence is a comprehensive approach to data security. As opposed to a set of specific technological standards, a broader, comprehensive approach has a better chance of retaining relevance over time while providing clearer guidelines than a vague reasonableness standard.[163] The Massachusetts data protection law[164] serves as an excellent example. As discussed above, federal laws and many state laws require

158. Sam Pfeifle, *Amidst U.S. Gov't Shutdown, State AGs Chuckle at Idea of Federal Breach Law,* The Privacy Advisor (Oct. 2, 2013), https://iapp.org/news/a/amidst-u.s.-govt-shutdown-state-ags-chuckle-at-idea-of-federal-breach-law.

159. *Id.*

160. Cory Bennett, *State AGs Clash with Congress over Data Breach Laws,* The Hill (Jul. 7, 2015), http://thehill.com/policy/cybersecurity/247118-state-ags-warn-congress-against-preempting-data-breach-laws/.

161. *Hogan Lovells' IAPP Tracker Post Highlights State Data Security Laws,* Hogan Lovells Chronicle of Data Protection (Dec. 22, 2014), http://www.hldataprotection.com/2014/12/articles/cybersecurity-data-breaches/hogan-lovells-iapp-tracker-post-highlights-state-data-security-laws/.

162. *See infra* Section IV.B.ii.

163. *See infra* Section IV.B.ii.

164. 201 Mass. Code Regs. 17.03-.04 (2010).

only reasonable security measures.[165] The Massachusetts law takes things a step further with a comprehensive approach that imposes stricter requirements on companies that collect consumer data.[166] While this law still uses a reasonableness standard, it is much more explicit as to what "reasonable" means.[167]

Specifically, the Massachusetts law requires any entity that collects personal information[168] of a Massachusetts resident to "implement a written information security program ('WISP') with appropriate administrative, technical, and physical safeguards."[169] Each WISP must include the following best practices:

1. The designation of at least one employee to maintain the WISP;
2. The assessment of risks to the security of records containing personal information, and improvement of safeguards to mitigate such risks, including employee training and detection and prevention of security system failures;
3. Disciplinary measures for violations of the WISP and safeguards for preventing terminated employees from accessing records containing personal information;
4. The development of security policies for the storage, access, and transportation of records containing personal information outside of business premises;
5. The implementation of reasonable restrictions upon physical access to records containing personal information, and the storage of such records and data in locked facilities, storage areas, or containers;
6. Monitoring the WISP's effectiveness in preventing unauthorized access to or use of personal information;
7. The review of the scope of the security measures at least annually or whenever there is a material change in business practices that may

165. *Supra* Section II.B.

166. *See* 201 Mass. Code Regs. 17 (2010); Kevin D. Lyles, et. al., *Massachusetts Law Raises the Bar for Data Security,* Jones Day (Feb. 2010), http://www.jonesday.com/massachusetts_law_raises/#_edn16.

167. 201 Mass. Code Regs. 17.03-.04 (mandating specific "standards for protecting personal information" and "computer system security requirements").

168. The Massachusetts law defines "personal information" as:

> *a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.* 201 Mass. Code Regs. 17.02 (2009).

169. Lyles, *supra* note 166.

reasonably affect the security or integrity of records containing personal information; and

8. The documentation of responsive actions to any security breach incidents and of post-incident review of events and actions taken to change business practices.[170]

Each WISP must also include a computer security program with "minimum standards for information security protocols."[171] Most significant of these standards is the duty to encrypt personal data,[172] which renders the information unreadable to those without use of confidential access.[173]

In addition to the WISP, the Massachusetts law requires companies to limit the amount of personal information that they collect. The collected information must be reasonably tailored to "accomplish the legitimate purpose for which it is collected."[174] Similarly, the companies must limit the amount of time that this information is stored to what is reasonably necessary.[175]

Furthermore, the Massachusetts law specifically addresses the issue of contracting with third-party service providers.[176] The statute requires that service providers be contractually bound to protect their systems on a basis consistent with the rest of the statute.[177] Therefore, even if a third-party service provider does not necessarily collect personal information itself, it is required to maintain a WISP and other security measures if it contracts with a company that does collect personal information.[178]

The Massachusetts law provides companies with clear guidelines as to what is considered "reasonable." In this way, it rises above current federal data protection

---

170. *Id.* (citing 201 Mass. Code Regs. 17.03(2) (2009)).

171. *Id.* These minimum security protocols include the following measures, to the extent they are technically feasible:

> *1. Secure control of user identifiers and passwords for authentication purposes; 2. Lock-out processes for inactive users or unsuccessful log-in attempts; 3. Limiting access to personal information to those persons who are reasonably required to know such information; 4. Up-to-date firewall protection and operating system security patches for systems connected to the Internet; 5. Up-to-date versions of system security agent software, including malware protection, patches, and virus definitions; and 6. Education and training of employees on the proper use of the computer security system. Id.*

172. *Id.;* The Massachusetts law defines "encrypt" as the "transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key." 201 Mass. Code Regs. 17.02.

173. Lyles, *supra* note 166.

174. *Id.*

175. *Id.*

176. 201 Mass. Code Regs. 17.03(2)(f).

177. *Id.* at 17.03(2)(f)(2).

178. *Id.*; This provision is modeled after a similar third-party service provider provision in the Gramm-Leach-Bliley Act. Lyles, *supra* note 166. As discussed in Section II.A.i above, the Gramm-Leach-Bliley Act only applies to financial institutions. *Supra.* The FTC has no such requirement under Section 5 of the Federal Trade Commission Act in its regulation of consumer economy. *See* 15 U.S.C. §§ 41-58 (2012).

laws and should be used as a model moving forward in protecting American consumers from data breaches and more specifically, third-party hacking.

ii. Attorney General Enforcement Power

Finally, Massachusetts gives its attorney general broad power to enforce the state's data protection law.[179] "Actions for injunctive relief and civil penalties of not more than $5,000 per violation (plus the reasonable costs of investigation and litigation) may be brought for any violations of the regulation."[180] The attorney general, as opposed to the FTC, is best suited to bring these enforcement actions. As one assistant attorney general put it, unlike the FTC, "(s)tate attorneys general hear directly from the residents they serve on a daily basis."[181] The same assistant attorney general went on to argue that a pre-emptive federal law "could place a wedge between consumers and the very state agencies that serve them."[182] Attorney generals are in the best position to enforce data protection laws and should be given broad power to do so.

V. Conclusion

Current federal data breach laws that focus primarily on the reasonableness of a company's security measures in light of its size are failing American consumers.[183] The vastly different data security plans of small and large companies are usually considered legal under the vague reasonableness standard.[184] This becomes an issue in third-party hacks, where hackers use weakly protected small businesses to infiltrate larger companies.[185] Using the Massachusetts data law as an example, states should pass more comprehensive data protection statutes.[186] These statutes must go beyond the reasonableness standard in providing clear guidelines as to what is expected of companies that collect consumer data, regardless of size, and give state attorney generals broad enforcement power if these expectations are not met.[187] In doing so, these state laws will be better suited to protect American consumers from having their personal information stolen as a result of third-party hackers.

179. Lyles, *supra* note 166.

180. *Id.* (citing *Mass. Gen. Laws* ch. 93A § 4 (2006)).

181. Erik C. Jones, *Step Aside, States?*, Slate (Jan. 22, 2015), http://www.slate.com/articles/technology/future_tense/2015/01/obama_data_breach_legislation_federal_laws_shouldn_t_pre_empt_state_laws.2.html.

182. *Id.*

183. *Supra* Section II.

184. *Supra* Section III.

185. *Supra* Section III.

186. *Supra* Section V.

187. *Supra* Section IV.