Campbell Law Review

Volume 42
Issue 1 *Winter 2020*

Article 7

2020

Protecting Personal Data: A Survey of Consumer Protections Throughout North Carolina's Identity Theft Protection Act

James H. Ferguson III

Protecting Personal Data: A Survey of Consumer Protections Throughout North Carolina's Identity Theft Protection Act

ABSTRACT

"Data is the pollution problem of the information age, and protecting privacy is the environmental challenge."[1]

You trade it every day. In a technologically-evolved world, our personal data has become a form of currency in the digital marketplace. Who is responsible for protecting that data? What happens when it is compromised? This Comment conducts a descriptive assessment of North Carolina's data breach notification law, exploring the legislative history of the Identity Theft Protection Act and comparing the consumer protections found therein to those offered in other states' statutory schemes. Additionally, this Comment evaluates the extent to which a statutorily required reasonable security standard comports with consumer protections, and their competitive interplay with businesses' economic interests.

1. BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 238 (W. W. Norton & Co., 1st ed. 2015).

INTRODUCTION

Your personal information is constantly at risk of falling into the wrong hands. Since 2005, over 10.4 billion data records have been compromised in over 9,000 data breaches in the United States.[2] A 2018 report predicts that more than "33 billion records will be stolen by cybercriminals in 2023 alone."[3] That report anticipates that the increase in breaches will significantly outpace business spending on data security.[4] Globally, data breaches affect about 25,575 people across the world, span a variety of industries, and cost organizations an average of $150 per record.[5]

The 2017 Equifax data breach, which exposed 143 million Americans' personal information—over a third of the country's population—was due to a vulnerability in the company's security system; a vulnerability known by the company two months prior to the record-setting breach.[6] More recently, affected consumers filed a class action lawsuit against Capital One for failing to take "reasonable care" in securing customers' personal information.[7] These recurring incidents beg the questions: how are businesses keeping our personal information safe and how are they being held accountable?

---

2. *Data Breaches FAQ*, PRIVACY RTS. CLEARINGHOUSE, https://perma.cc/E8YY-BQ9N.

3. *Cybersecurity Breaches to Result in Over 146 Billion Records Being Stolen by 2023*, JUNIPER RES. (Aug. 8, 2018), https://perma.cc/S595-KQDS [hereinafter *Cybersecurity Breaches*].

4. *Id.* (predicting the number of breached records will triple over the next five years while the annual spending on cyber security will only increase by an average of nine percent per company).

5. PONEMON INST. (with sponsorship from IBM SECURITY), COST OF A DATA BREACH REPORT 3, 16 (2019), https://perma.cc/QY63-VRWT.

6. *See* Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017), https://perma.cc/AZ8L-QC3M.

7. AJ Dellinger, *Capital One Hit with Class-Action Lawsuit Following Massive Data Breach*, FORBES (July 30, 2019), https://perma.cc/B3G5-TVEG.

When it comes to data security, businesses are regulated by a variety of frameworks.[8] These frameworks can be categorized into two groups: traditional legal frameworks and private ordering frameworks.[9] Private orderings are typically industry standards and contractual duties, while traditional legal frameworks are federal and state laws and regulations.[10] Among these regulations are data breach notification laws.[11]

Breach notification laws are designed to put consumers on notice of a potential threat to their personal information.[12] As of 2018, all fifty states have laws requiring private or governmental entities to disclose a security breach incident involving personally identifiable information of the states' residents.[13] These laws aim to protect consumers from actual economic injuries caused as a result of identity theft, as well as injuries to one's "dignitary" interest resulting from a violation of one's informational privacy.[14]

The difference between a consumer's economic interests and his or her dignitary interests is that the economic interest is concerned with the information associated with a consumer's financial resources (*e.g.*, bank accounts, PINs), whereas the dignitary interest is concerned with non-financial information (*e.g.*, health insurance, medical data).[15] Typically, these consumer interests compete with businesses' interests, and state governments are forced to make political judgements as to which interest they will elevate.[16] Analyzing to whom the state places the financial burden is the best indicator for which interest is at the heart of a breach notification statute.[17]

---

8. *See* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1141–43 (2019).

9. *See id.* at 1143, 1158.

10. *Id.* at 1142.

11. *Id.* at 1143.

12. *See generally* Sara A. Needles, Comment, *The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law*, 88 N.C. L. REV. 267 (2009); *see also* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 932 (2007) (describing "disclosure of information [as] a central regulatory tool"); Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS (July 12, 2018), https://perma.cc/6SFR-WT3H.

13. *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Sept. 29, 2018), https://perma.cc/FXQ9-F56D.

14. Needles, *supra* note 12, at 271.

15. *Id.* at 280–87.

16. *Id.* at 271.

17. *See generally* Paul Rosenzweig, *Cybersecurity and the Least Cost Avoider*, LAWFARE (Nov. 5, 2013), https://perma.cc/3MWK-YJ8U (explaining the economic principle that the party best able to insure against an event should bear that economic burden).

Currently, only about half the states have laws addressing private businesses' data security practices,[18] but all fifty states have security measures in place aimed at protecting the state's own data and information systems.[19] At least twenty-nine states statutorily require their government agencies to have reasonable security measures in place to ensure the security of the states' data systems.[20] For example, in 2015, North Carolina established the role of State Chief Information Officer ("CIO").[21] One of the CIO's primary responsibilities is to "ensure the security of State information technology systems . . . [and] associated data" through statewide security standards.[22] Many states have adopted these types of measures because state systems are appealing targets to cybercriminals due to the massive amounts of data they store on each of the states' residents.[23] In spite of the increasing amounts of data businesses collect and retain, state legislatures are slow to apply these same standards to the private sector.[24] This suggests a strong preference in protecting businesses' interests over those of the consumers; however, that trend seems to be changing.

State legislatures across the country are grappling with what role they play in securing residents' personal information in the hands of private entities,[25] attempting to balance consumers' interests in securing their information with businesses' concerns over raised compliance costs. With regulations like those enacted under the California Consumer Privacy Act

18. *Data Security Laws-Private Sector*, NAT'L CONF. ST. LEGISLATURES (May 29, 2019), https://perma.cc/9DFE-GLPM.

19. *Data Security Laws-State Government*, NAT'L CONF. ST. LEGISLATURES (Feb. 22, 2019), https://perma.cc/8GDE-VRJE.

20. *Id.*

21. Act of Sept. 18, 2015, No. 2015-241, § 7A.2(b), 2015 N.C. Sess. Laws 671, 671–93 (amending Chapter 143B of the N.C. General Statutes to include a new article: Article 14).

22. N.C. GEN. STAT. § 143B-1322 (2017) (prescribing the duties of the State's CIO, which includes ensuring the security of the State's information technology systems).

23. *See Data Security Laws-State Government*, *supra* note 19.

24. While traditional grammarians will point out that data is the plural form of the singular word datum, the "semantic bleaching" of the word data over time has caused it to be accepted as singular. This Comment will take that more contemporary meaning of the word data, referring to it as the singular "collection of information in aggregate." Daniel Oberhaus, *It's Time to End the "Data Is" vs. "Data Are" Debate*, VICE: MOTHERBOARD (Aug. 20, 2018), https://perma.cc/GD86-HTLT (internal quotation marks omitted).

25. At the start of the 2019 legislative session, forty-three states and Puerto Rico "introduced or considered close to 300 bills or resolutions that deal significantly with cybersecurity." *Cybersecurity Legislation 2019*, NAT'L CONF. ST. LEGISLATURES (Sept. 16, 2019), https://perma.cc/64DG-YKFE. Additionally, while all fifty states have some form of a data breach notification law, at least thirty-one states have considered measures that would amend existing breach laws. *Id.*

("CCPA")[26] and the New York Stop Hacks and Improve Electronic Data Security ("SHIELD") Act,[27] combined with the extra-territorial privacy rights recognized by the European Union's General Data Protection Regulation ("GDPR"),[28] states are looking to address the weaknesses in their own laws, all while Congress considers preemptive measures in this widely unregulated area of the law.[29]

States that have chosen to regulate private businesses' data security measures "require businesses that own, license, or maintain personal information about a resident of that state to implement and maintain '*reasonable* security procedures and practices' appropriate to the nature of the information and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[30] The number of states that statutorily require these measures has "doubled since 2016, reflecting growing concerns" about cybercrimes and personal information breaches.[31]

In the 2019 North Carolina Legislative session, representatives from both sides of the aisle introduced the Identity Theft Protection Act/Changes, a bill that attempted to place that same reasonableness standard on private businesses.[32] Though less prescriptive than the California state law, the proposed North Carolina legislation would have placed an increased level of responsibility on businesses that handle residents' personal data.[33] While these legislative efforts failed, this topic remains a debate in state legislatures across the country.[34] This Comment will compare the proposed

26. S.B. 1121, 2018 Leg. (Cal. 2018).

27. S.B. 5575-B, 2019 N.Y. S., 2019–2020 Reg. Sess. (N.Y. 2019).

28. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter Regulation 2016/679].

29. *See* Abbie Gruwell, *Preemption Takes Center Stage Amid Federal Data Privacy Action*, NAT'L CONF. ST. LEGISLATURES (Apr. 8, 2019), https://perma.cc/7VEK-CTP6.

30. *Data Security Laws-Private Sector*, *supra* note 18 (emphasis added). The proposed North Carolina legislation contained language identical to this general reasonableness requirements. H.B. 904, 2019 Gen. Assemb. (N.C. 2019).

31. *Id.*

32. The bill stated in part that "[a]ny business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form . . . shall . . . [i]mplement and maintain *reasonable* security procedures and practices." *Id.* (emphasis added); *see also* Adam Bridgers & Fisher Phillips, *Strict Privacy and Data Security Bill Introduced in North Carolina*, JDSUPRA (May 13, 2019), https://perma.cc/MP3K-4JXK.

33. *See* Bridgers & Phillips, *supra* note 32.

34. *Id.*

legislation of House Bill 904 to other states' statutes and analyze its compatibility with North Carolina's existing statutory interests.

This Comment will forego making normative judgements about the proposed legislative scheme, but rather will conduct a descriptive assessment of North Carolina's protections. Part I will examine North Carolina's existing statutory protections and will establish two propositions: that these protections (A) are situated to address consumers' purely economic interests, and (B) tend to favor minimizing businesses' cost of compliance.[35] Part II will evaluate the proposed reasonableness standard for data security against the backdrop of these consumer and business interests. Part III concludes.

I. NORTH CAROLINA'S STATUTORY INTERESTS

Many states, including North Carolina, elect to solely protect consumers' economic interests, while others extend their statutory protections to include consumers' dignitary interests.[36] By adopting this dichotomy and applying it to North Carolina's Identity Theft Protection Act, this Part will establish the following propositions: (A) North Carolina's law only protects consumers' economic interests, as opposed to their dignitary interests, associated with "information privacy,"[37] and (B) North Carolina's law tends to impose less costs on businesses, so as to protect their economic interests.

A. Protecting Consumer Economic Interests

Historically, the state has always sought to only protect the type of information that could be used to cause the consumer direct financial harm, what this Comment will refer to as the consumer's economic interest.[38] In analyzing the legislative history of the state's Identity Theft Protection Act as well as the definition of "personal information" used in that article, this Part will demonstrate that proposition.

1. Legislative History of the Identity Theft Protection Act

As the state legislature has amended the state's identity theft statutory protections over time, consumers' economic interests remained at the heart of those protections.[39] In 1999, North Carolina created the criminal offense

35. Needles, *supra* note 12, at 271.

36. *Id.* at 281, 286.

37. *See id.*

38. *Id.* at 281.

39. *See* N.C. GEN. STAT. § 75-66 (2017).

of "Financial Identity Fraud,"[40] a specific-intent crime that involved the use of an individual's personal information to fraudulently represent oneself as the individual in a financial or credit transaction.[41] A few years later, the General Assembly removed the intent requirement from the criminal statute and added a private right of action, providing up to $5,000 in damages or trebled damages, whichever was greater.[42] This early form of what we now refer to as "identity theft" was solely meant to protect individuals from losing their financial resources. The later-added private right of action utilized punitive measures to further protect consumers' economic interests.[43]

In 2005, the General Assembly renamed the offense, changing the name from "Financial Identity Fraud" to "Identity Theft," and placed a duty on businesses to report a security breach involving their customers' personal identifiable information.[44] This disclosure requirement was consistent with multiple sector-specific federal laws passed years earlier aimed at protecting consumers' private information—both financial and dignitary.[45] In

40. Act of Aug. 10, 1999, No. 1999-449, § 1, 1999 N.C. Sess. Laws 1813, 1813–14. During this time, many states created similar offenses, in part due to the federal government recognizing identity theft as a federal crime because of the rise of the practice with the advent of the Internet. KRISTIN FINKLEA, CONG. RESEARCH SERV., R40599, IDENTITY THEFT: TRENDS AND ISSUES 4 (2014) (citing Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (1998)).

41. § 1, 1999 N.C. Sess. Laws at 1813. Additionally, at that time, North Carolina's law focused solely on punishing and deterring those individuals gaining access to consumers' information rather than addressing the reasons that such personal information was vulnerable to theft and fraud in the first place. Committing financial identity fraud was a Class H felony unless the victim suffered "arrest, detention, or conviction as a proximate result of the offense," which was then a Class G felony. *Id.* (codifying "Punishment and liability" for this violation at N.C. GEN. STAT. § 14-113.22 (2017)).

42. Act of Oct. 31, 2002, No. 2002-175, § 8, 2002 N.C. Sess. Laws 786, 790. This session law also expanded the definition of "identifying information" to include biometric data, fingerprints, passwords, and parents' legal surnames prior to marriage. § 4, 2002 N.C. Sess. Laws at 788. Three years later the legislature expanded the definition to include ID and passport numbers, email addresses or names, and other Internet account identifiers. Act of Sept. 21, 2005, No. 2005-414, § 6, 2005 N.C. Sess. Laws 1547, 1560–61.

43. *Id.* at 1562 (providing for trebled damages to consumers who suffered actual harm as a result of the crime).

44. Act of Sept. 21, 2005, No. 2005-414, § 1, 2005 N.C. Sess. Laws 1547, 1554–56 (amending the statutes to include N.C. GEN. STAT. § 75-65 (2017)). Three years earlier, California became the first state to require businesses to notify its customers of a security breach involving their personal information. *See* FINKLEA, *supra* note 40, at 21.

45. Congress passed the Gramm-Leach-Bliley ("GLB") Financial Services Modernization Act in 1999, which regulated the collection and use of consumers' information. The Act required notice on financial institutions information-disclosure practices. Additionally, in 2001, Congress passed similar measures for the health care industry—the Health Insurance Portability and Accountability Act ("HIPAA")—and its security rules regulated the use

requiring notice to affected consumers, North Carolina narrowly defined "personal information" to only include information that could be used to access an individual's financial resources.[46]

This legislative history evinces the legislature's hesitation to extend consumer protections beyond the traditional financial protections.

2. Current Statutory Definition of "Personal Information"

North Carolina's current identity theft protection: (1) requires businesses to implement *reasonable measures* when destroying records with residents' personal information; (2) requires breached businesses to notify affected consumers of a security breach; and (3) prohibits the publication of personal information.[47] A violation of either of the first two protections is a *per se* violation of the state's Unfair and Deceptive Trade Practices ("UDTP"), granting the consumer a private right of action for actual harm caused with the allowance for trebled damages.[48] A violation of the last is eligible for the same remedies; however, it is not considered an UDTP.[49]

The first and third protections differ from the second in how they define "personal information." Generally, state statutes define "personal information" as an individual's first name or initial and last name in addition to one or more of the following data elements:

1. Social Security number ("SSN");
2. Driver's license number or state-issued ID-card;
3. Account number, credit or debit card number combined with any security or access code, PIN or password needed to access an individual's financial account.[50]

---

of unique identifiers related to the physical or mental health of an individual. *See generally* Fred H. Cate, *The Privacy Problem: A Broader View of Information Privacy and the Costs and Consequences of Protecting It*, 4 FIRST REP., no. 1, Mar. 2003, at 6–10 (discussing the GLB Act and HIPAA, along with the Children's Online Privacy Protection Act of 1998 and the Driver's Privacy Protection Act of 1994).

46. *See* N.C. GEN. STAT. § 75-61(10) (2017) (incorporating N.C. GEN. STAT. § 14-113.20(b) by reference); *see also infra* Section I.A.2.

47. N.C. GEN. STAT. §§ 75-60–75-66 (2005).

48. N.C. GEN. STAT. §§ 75-62(d), -63(q), -63.1(g), -64(f), -65(i) (2017) (referencing N.C. GEN. STAT. § 75-1.1); *see generally* Matthew W. Sawchak, *Refining Per Se Unfair Trade Practices*, 92 N.C. L. REV. 1881 (2014).

49. *See* N.C. GEN. STAT. § 75-66(e) (referencing N.C. GEN. STAT. § 1-539.2C) (describing "[d]amages for identity theft," which allow for treble damages or damages between $500 and $5,000, whichever is greater).

50. *See* FLA. STAT. § 501.171(1)(g) (2018); GA. CODE ANN. 10-1-911(6) (2017); N.Y. GEN. BUS. § 899-aa(1)(a)–(b) (McKinney & Supp. 2019) (as amended S.B. 5575-B, 2019

North Carolina's statutory definition extends this general definition to include a variety of other data elements.[51] However, North Carolina specifically excludes these additional data elements from its definition of personal information for the purpose of its breach notification law.[52] This exclusion limits the types of data that triggers notification in the event of a data breach, and directly limits the protection to information that could be used to cause measurable economic harm. Many surrounding states have similar definitions that seek to protect data that would provide access to a resident's financial accounts, which could cause the economic harm the statute seeks to protect against.[53] Some states have extended their definition to include medical and health information, as well as internet identification numbers and email addresses, which could cause economic or dignitary harms.[54] By extending a definition to include these non-financial based data elements, a state protects beyond the traditional economic interests.

A state that extends consumer protections to include dignitary interests in its breach notification law places a higher cost burden on businesses that maintain or possess that particular type of data. In other words, if non-financial data is the subject of a breach, then the business maintaining that data is on the hook for paying the cost of notifying its customers, in spite of the fact that the data may not cause economic harm.[55] States—like North Carolina—that narrowly define personal information for breach-

N.Y. S., 2019–2020 Reg. Sess. (N.Y. 2019)); S.C. CODE ANN. § 39-1-90(D)(3) (2018); TENN. CODE ANN. § 47-18-2107(a)(4)(A)(i)–(iii) (2013).

51. *See* N.C. GEN. STAT. § 75-61(10) (incorporating N.C. GEN. STAT. § 14-113.20(b) by reference, which includes electronic identification numbers, biometric data, fingerprints, and parents' legal surname before marriage).

52. N.C. GEN. STAT. § 75-65(a) (stating "unless this information would permit access to a person's financial account or resources.").

53. *See* FLA. STAT. § 501.171(1)(g); GA. CODE ANN. § 10-1-911(6); S.C. CODE ANN. § 39-1-90(D)(3); TENN. CODE ANN. § 47-18-2107(a)(4).

54. *See* CAL. CIV. CODE § 1798.82(h)(1)–(2) (2017) (including usernames and email addresses "in combination with a password or security question and answer" in order to access a resident's financial account; information collected through the use of an automated license plate recognition system; and medical information); MD. CODE ANN., COM. LAW § 14-3501(d)(2) (West 2013); N.Y. GEN. BUS. § 899-aa(1)(a)–(b) (as amended S.B. 5575-B, 2019 N.Y. S., 2019–2020 Reg. Sess. (N.Y. 2019)). New York's recently passed SHIELD Act expands the state's definition of "private information" to include many of the data elements North Carolina's statute already lists; however, New York has maintained those elements for the state's breach notification statute. N.Y. GEN. BUS. § 899-aa(1)(a)–(b) (as amended S.B. 5575-B, 2019 N.Y. S., 2019–2020 Reg. Sess. (N.Y. 2019)); *see also* Mark Krotoski & Martin Hirschprung, *Preparing for the New Data Breach and Security Requirements Under the New York SHIELD Act*, N.Y. L.J. (Oct. 1, 2019), https://perma.cc/FVG3-PRZY.

55. *See* Krotoski & Hirschprung, *supra* note 54.

notification purposes are solely protecting residents' economic injuries while managing businesses' cost burden.[56]

The legislative history of North Carolina's identity theft protections and the narrow definition of personal information affirm the proposition that the statutes seek to protect consumers' purely economic interests.

B. North Carolina's Law and Increasing Costs on Businesses

The next step in applying the breach notification framework is to weigh these purely economic, consumer interests against those of businesses that operate in the state and are subject to compliance with the statutory protections.[57] The balance between consumer and business interests is dependent on the scope of the breach and the required notice.[58]

1. Scope of the Breach

North Carolina defines "security breach" as "[a]n incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer."[59] This definition narrowly limits notification to access *and* acquisition of the protected data, requires a risk analysis, and only applies to unencrypted data.

i. Access and/or Acquisition

Generally, most states define a "security breach" as the "unauthorized access to *and* acquisition of" the statutorily protected data.[60] Few states broaden this definition to the unauthorized access *or* acquisition of the protected data.[61]

---

56. Kerry, *supra* note 12 (arguing the focus of the state's definition is too narrow, because "[t]he aggregation and correlation of data from various sources make it increasingly possible to link supposedly anonymous information to specific individuals and to infer characteristics and information about them").

57. Needles, *supra* note 12, at 273–75.

58. *Id.*

59. N.C. GEN. STAT. § 75-61(14) (2017).

60. *Id.*; *see, e.g.*, S.C. CODE ANN. § 39-1-90(D)(1) (2019); VA. CODE ANN. § 18.2-186.6(A) (2014) (emphasis added); *see also* BAKER & HOSTETLER, DATA BREACH CHARTS (2018), https://perma.cc/683V-6NG5.

61. CONN. GEN. STAT. § 36a-701b(a) (2019); N.J. STAT. ANN. § 56:8-161 (West 2012); N.Y. GEN. BUS. § 899-aa(1)(c) (as amended by S.B. 5575-B, 2019 N.Y. S., 2019–2020 Reg. Sess. (N.Y. 2019)).

By extending the definition of security breach to the disjunctive—access *or* acquisition[62]—a state broadens its consumers' economic protections because the breach law would encompass more incidents that would trigger a business's duty to notify.[63] This extended definition benefits consumers' economic interests because it provides them with notice of any type of incident that could have potentially compromised their data, thus allowing them to more readily monitor their financial information. However, frequent notifications in "'non-threatening situations'" likely weakens the effectiveness of this type of protection and increases the businesses' cost of compliance.[64]

ii. Risk-Of-Harm Analysis

Some states require a risk-of-harm analysis to determine when businesses must notify affected consumers.[65] In determining whether the compromised data "creates a material risk of harm to a consumer,"[66] a business must analyze the information subject to the breach. A consequence of this investigation requirement is that businesses may delay notice to the affected consumers to give the businesses time to analyze the breached records, thereby delaying the economic harm to the "reputational capital" of the businesses.[67] While businesses are able to avoid these reputational harms, consumers are subjected to the unnecessary risk that their personal information will be used in the meantime.[68]

---

62. To access something means "to be able to use, enter, or get near (something)," while to acquire it means "to come into possession or control of often by unspecified means." *Access,* MERRIAM-WEBSTER, https://perma.cc/U72W-ZAJS; *Aquire*, MERRIAM-WEBSTER, https://perma.cc/87VN-5T7X. The difference is the potential to possess versus actual possession. In terms of a data breach, to access data is to have the ability to use the data, while to acquire the data means to have it in your possession. This line is especially blurred given the fact that data, itself, is not tangible.

63. "[W]hen compared to acquire, [access] is clearly a lower standard . . . ." Jim Harvey et al., *Key Data Breach Jurisdictions: An Analysis*, ALSTON & BIRD: CYBER ALERT (Jan. 11, 2013), https://perma.cc/SCR5-BPTP.

64. Schwartz & Janger, *supra* note 12, at 939 (quoting Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,740 (Mar. 29, 2005)); *see generally* Cate, *supra* note 45, at 22–25 (addressing the businesses' cost to provide notice).

65. *See, e.g.*, FLA. STAT. § 501.171(4)(c) (2018); MD. CODE ANN., COM. LAW § 14-3504(a)(1), (b)(2) (LexisNexis through 2019); S.C. CODE ANN. § 39-1-90(D)(1) (2018); TENN. CODE ANN. § 47-18-2107(a)(1)(A) (2013); VA. CODE ANN. § 18.2-186.6(B).

66. N.C. GEN. STAT. § 75-61(14) (2017).

67. Schwartz & Janger, *supra* note 12, at 929.

68. "The longer an instance of identity theft goes undetected, the greater the damage that usually follows." Schwartz & Janger, *supra* note 12, at 942 (citing SYNOVATE, FED.

iii. Encryption Safe Harbors

Many states only require businesses to notify affected consumers of a breach if the information subject to the breach was unencrypted or unredacted.[69] This carve-out is known as an "encryption safe harbor."[70] North Carolina, like many states, defines encryption to mean "[t]he use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key."[71] North Carolina defines redaction to mean "[t]he rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number is accessible as part of the data."[72] North Carolina, along with a handful of states, also extends the duty to notify affected individuals to encrypted data, but only if the key or process to unencrypt it was also subject to the breach.[73]

Exempting encrypted or redacted data from a state's breach notification law incentivizes businesses to take these types of protective measures to ensure collected data is secure.[74] This encryption exemption is indicative of the legislature balancing both the consumers' interest in data protection and businesses' interest in lower compliance costs.[75] On the other hand, technological advances in decryption could create a notification gap for states that offer such encryption safe harbors.[76] That is, if notification is not required for compromised encrypted data and the hacker can decrypt the

---

TRADE COMM'N IDENTITY THEFT SURVEY REPORT 8 (Sept. 2003), https://perma.cc/4VL6-F3DW).

69. *Compare* FLA. STAT. § 501.171(g)(2); MD. CODE ANN., COM. LAW §14-3501(d)(1) (also applying the safe harbor when the information is "otherwise protected by another method"), *and* S.C. CODE ANN. § 39-1-90(A) (also allowing "other methods" of making data unreadable) *with* CAL. CIV. CODE § 1798.82(a) (2017); N.C. GEN. STAT. § 75-61(14); TENN. CODE ANN. § 47-18-2107(a)(1)(A)(i); VA. CODE ANN. §18.2-186.6(A) (requiring unencrypted and unredacted).

70. BAKER & HOSTETLER, *supra* note 60, at 28–31.

71. N.C. GEN. STAT. § 75-61(8).

72. N.C. GEN. STAT. § 75-61(13).

73. *See, e.g.*, N.C. GEN. STAT. § 75-61(14); TENN. CODE ANN. § 47-18-2107(a)(1)(A)(ii); VA. CODE ANN. § 18.2-186.6(C).

74. *See* Mark Burdon, *Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 63, 89 (2010).

75. *See id.*

76. *See* Catherine Stupp & James Rundle, *Capital One Breach Highlights Shortfalls of Encryption*, WALL ST. J. (Aug. 2, 2019), https://perma.cc/FWY5-WGHR; *see also Google Claims to Have Demonstrated "Quantum Supremacy,"* ECONOMIST (Sept. 28, 2019), https://perma.cc/6ML3-QT7K (describing how "a quantum machine could quickly untangle the complex math that underlies much of the scrambling that protects information online").

encrypted data, then those consumers' data is exposed to potential financial damages but remain unnotified of the breach because their data was initially encrypted.

North Carolina's narrow definition of security breach, which includes a risk analysis, protects consumers from frivolous notifications.[77] The state's encryption safe-harbor protects consumers' data by incentivizing businesses to invest in at least one element of a reasonable data security practice, while managing the cost to businesses.[78] This strikes a balance between consumers' purely economic interests and the interests of the state's businesses.

2. Notice Requirements

Notice is fundamental in alerting a consumer to a potential threat of misuse of their personal information.[79] Scholars are split as to its value in protecting consumers' interests, as "compliance is often conflated with effectiveness."[80] Key components to notice are timing and form.[81]

i. Timing of Notice

Generally, notice is required in the most expedient time and manner possible, without unreasonable delay, but consistent with the needs of law enforcement.[82] Some states specify a time frame for when notice is to be served.[83] A time frame for notice supports consumers' interests by providing them with timely notice; a lack of a definite time frame supports businesses' interest in providing more time to comply—and ultimately less cost.

77. *See* N.C. GEN. STAT. § 75-61(14).

78. *See* Burdon, *supra* note 74.

79. Schwartz & Janger, *supra* note 12, at 932 ("[D]isclosure of information is a central regulatory tool").

80. Needles, *supra* note 12, at 272.

81. *Id.* at 275 ("Whether or not unauthorized access in any of these cases triggers a duty to notify depends on three key variables in state notification laws[.]" These variables are "the statute's definition of 'personally identifiable information,' the statute's scope and whether it includes a risk-based exception, and the form and timing of notice the statute prescribes.").

82. *See, e.g.*, CAL. CIV. CODE § 1798.82(a) (2017); GA. CODE § 10-1-912(a) (2017); N.Y. GEN. BUS. § 899-aa(2) (McKinney & Supp. 2019) (as amended S.B. 5575-B, 2019 N.Y. S., 2019–2020 Reg. Sess. (N.Y. 2019); N.C. GEN. STAT. § 75-65(a)–(b); S.C. CODE ANN. § 39-1-90(A) (2018); VA. CODE ANN. § 18.2-186.6(D) (2014).

83. For example, Florida requires notice be given to affected consumers within thirty (30) days from the time a breach is discovered, while Maryland and Tennessee require it within forty-five (45) days. FLA. STAT. § 501.171(4)(a) (2018); MD. CODE ANN., COM. LAW § 14-3504(b)(3) (West 2013); TENN. CODE ANN. § 47-18-2107(b) (2013).

North Carolina requires businesses that own or license personal information to give notice of the breach "without *unreasonable* delay."[84] Businesses which maintain personal information of North Carolina residents and do *not* own or license the information must give notice "*immediately* following discovery of the breach, consistent with the legitimate needs of law enforcement[.]"[85]

Most states allow for a delay in notification for "the legitimate needs of law enforcement."[86] Such a delay in notice is a rational policy judgment of favoring the general public's interest in apprehending a criminal hacker at the expense of the individual victims' interest in protecting the victims' financial resources.[87] An unintended consequence of this type of delay is that it allows businesses to delay publicly disclosing information about their security incident.[88] Although it is an unintended consequence, a delay in public disclosure saves businesses the losses associated with reputational sanctions.[89]

ii. Forms of Notice

Typically, states allow for businesses to provide written, electronic, or telephonic notice to consumers affected by a data breach.[90] State statutes typically prescribe the information that must be provided to constitute adequate notice, generally including the breached business's identity.[91] In requiring this type of "particularized" notice, states seek to impose a reputational sanction on breached businesses—along with the cost of notice.[92] These types of notice focus on publicly shaming the breached businesses for their lax data security standards.[93] Additionally, this notice ensures

84. N.C. GEN. STAT. § 75-65(a) (emphasis added).

85. N.C. GEN. STAT. § 75-65(b) (emphasis added).

86. For example, see *id.* at § 75-65(a)–(b).

87. Schwartz & Janger, *supra* note 12, at 942.

88. *Id.* (discussing the Los Angeles police department's investigation into ChoicePoint for delaying their disclosure after police cleared the company to share the information).

89. *Id.* at 929–32.

90. *See, e.g.*, FLA. STAT. § 501.171(4)(d) (2018) (prohibiting, by inference, telephonic notice); GA. CODE ANN. § 10-1-911(4) (2017); MD. CODE ANN., COM. LAW § 14-3504(e) (LexisNexis through 2019); N.C. GEN. STAT. § 75-65(e); S.C. CODE ANN. § 39-1-90(E) (2018); TENN. CODE ANN. § 47-18-2107(e) (2013); VA. CODE ANN. § 18.2-186.6(A) (2014).

91. *See, e.g.*, N.C. GEN. STAT. § 75-65(d).

92. Schwartz & Janger, *supra* note 12, at 936 (comparing models of notice with respect to reputational information).

93. "The statute's insight is that disclosure causes a useful embarrassment: to avoid notice and the accompanying reputational loss, a business will invest ex ante in data security

individual consumers are put on alert that their information may have been compromised and allows them to effectively monitor their own financial interests. These forms of notice comport with the statute's interest in protecting the consumer's financial interest.[94] Still, many states carve out a cost exemption for businesses in the form of substitute notice.[95]

Substitute notice is acceptable if the cost to the business or the number of affected people to be notified exceeds a particular statutory threshold.[96] By allowing this type of notice, states shift the cost associated with monitoring and mitigating the harms, as a result of the breach, from the breached businesses to the affected consumers. Substitute notice still brings the same reputational harms associated with a massive data breach. However, it does not address the consumers' financial interests because substitute notice does not require individual consumer notification. Therefore, some consumers will be unaware that their information has been compromised and will be unable to self-protect from the harms associated with the breach.[97] Additionally, substitute notice allows businesses to save on the cost of notifying each individual and to opt for a more affordable option.[98]

Ultimately, the regime of notice requirements found in states' statutes, including North Carolina's statutes, demonstrates how the state favors business interests—at times, at the expense of the consumers' economic interests. However, the definitions of personal information and security breach support the consumers' interests while minimizing costs to businesses. These measures are reactive, rather than proactive. The next Part applies the same framework to the implementation of a statutory reasonableness standard and discusses the feasibility of this standard in the state's current statutory structure.

---

and, ex post, will respond more effectively and vigorously to a breach due to increased public and regulatory scrutiny of its practices." *Id.*

94. *See* Needles, *supra* note 12, at 288–89.

95. *See, e.g.*, GA. CODE ANN. § 10-1-911(4)(D); MD. CODE ANN., COM. LAW § 14-3504(e)(4); N.C. GEN. STAT. § 75-65(e)(4); S.C. CODE ANN. § 39-1-90(E)(4); TENN. CODE ANN. § 47-18-2107(e)(3); VA. CODE ANN. § 18.2-186.6(A).

96. For many of the Southeastern states, the cost of notice must exceed $250,000 or the number of affected people must exceed 500,000 for a business to deploy substitute notice of a data breach. *See* FLA. STAT. §501.171(4)(f) (2018); N.C. GEN. STAT. §75-65(e)(4); S.C. CODE ANN. §39-1-90(E)(4); TENN. CODE ANN. §47-18-2107(e)(3).

97. *See* Schwartz and Janger, *supra* note 12, at 936.

98. This can be seen in the statutory cost of notice thresholds in state statutes, such as New Jersey, Iowa, and Rhode Island. Needles, *supra* note 12, at 288–89.

II. THE "REASONABLE SECURITY PROCEDURES" STANDARD

Once the State adopts a reasonableness standard for private businesses, the next question is: what exactly constitutes a *reasonable* security procedure?[99] In the absence of federally-mandated standards of security, and a patchwork of state regulations, the concept of reasonableness is "notoriously vague," often turning "on [the] whims of the fact-finder for highly case-specific reasons."[100] Additionally, the standard changes on a sliding scale relative to "the nature of the data held by the business."[101] This flexible standard is appealing to many lawmakers and regulators because it does not prescribe rigid requirements that are unduly burdensome to businesses, particularly small businesses.[102] Of the states that have passed data security requirements for businesses, none have explicitly defined what procedures constitute a "reasonable" measure.[103]

Aside from federal and state industry-specific guidelines for entities' security standards,[104] many states with this type of reasonable requirement, leave the interpretation up to the regulated entity. On the broadest end of the spectrum, Maryland simply requires businesses to "implement and maintain *reasonable* security procedures and practices," similar to the proposed language of the North Carolina legislation.[105] On the more detailed side, Ohio's statute requires businesses' cybersecurity programs to contain "administrative, technical, and physical safeguards for the protection of personal information and that reasonably conforms to an industry recognized

---

99. Philip N. Yannella, *What Does "Reasonable" Data Security Mean, Exactly?*, BALLARD SPAHR LLP: CYBERADVISER (Jul. 20, 2018), https://perma.cc/A4VA-JH6M; *see also* Paul Otto & Brian Kennedy, *"Reasonable Security" Becomes Reasonably Clear to the California Attorney General*, HOGAN LOVELLS: CHRON. DATA PROTECTION (Mar. 1, 2016), https://perma.cc/6V36-6W67.

100. Yannella, *supra* note 99.

101. *Id.*; *see* Dellinger, *supra* note 7 (discussing the controversies over "adequate measures" in the Capital One breach).

102. Yannella, *supra* note 99.

103. *Id.*

104. On the federal level, GLB and HIPAA prescribe standards that financial institution and healthcare businesses must implement to maintain the security of the consumers within those industries. *See* 16 C.F.R. § 314.4 (2019); 45 C.F.R. § 164.530 (2018). Additionally, South Carolina applies a specific set of safety procedures for individuals licensed by the state's insurance laws. *See* S.C. CODE §§ 38-99-10 to -100 (2019) (as amended by 2018 H.B. 4655). New York's Cybersecurity Requirements for Financial Services Companies requires entities to implement a security program, based on risk assessments that address a host of the entities' daily operations. N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2018).

105. MD. CODE ANN., COM. LAW § 14-3503(a) (LexisNexis through 2019) (emphasis added).

cybersecurity framework."[106] The statute later outlines what constitutes acceptable industry standards.[107]

The theory behind a vague reasonableness standard, according to some legislators and regulators, is that the definition of reasonable "will be fleshed out by future courts and through regulatory enforcement actions."[108] Although the courts have yet to define reasonableness in this respect,[109] the Federal Trade Commission ("FTC") has acted, under its authority to investigate unfair trade practices, as a mechanism for defining what the government may see as an acceptable set of reasonable standards in this area.[110] Businesses have had to adapt their security measures in order to conform with a number of legal and private frameworks, including the FTC's regulations, establishing a groundwork for what constitutes as "reasonable."[111]

106. OHIO REV. CODE ANN. § 1354.02(A)(1) (Westlaw through 133rd General Assemb.). Using industry standard-based guidelines to determine reasonableness may be a more desirable approach for fields that are constantly evolving.

107. OHIO REV. CODE ANN. § 1354.03 (Westlaw through 133rd General Assemb.).

108. Yannella, *supra* note 99.

109. "To date, none of the data breach class actions that have proceeded past the summary judgment phase has litigated to judgment the issue of reasonableness." *Id.*

110. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 583 (2014); *see* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 293 n.18 (2014); *see also* McGeveran, *supra* note 8, at 1182 (discussing David Thaw's "'Management-Based Regulatory Delegation,'" in which "government authorities mandate that companies develop internal regulations . . . concerning data security").

111. "Regulated parties are already shaping their data security measures in response. Like most businesses, they try to do so with common sense: they weigh costs and benefits, assess risk, and invest accordingly." McGeveran, *supra* note 8, at 1137 (citing KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 27–33 (Sandra Braman & Paul Jaeger eds., 2015)).

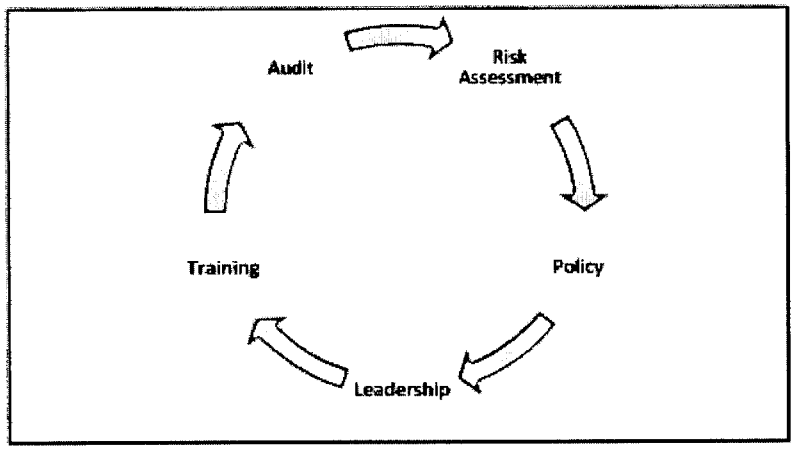

Figure 1: A typical business compliance system.[112]

Data security should be viewed "as a process, not a product."[113] The process begins with a risk assessment, which includes mapping the flow of information and where vulnerability exists within that system.[114] After the risk assessment is complete, a formal policy should be created to address the identified risks.[115] This policy, and its compliance, should be internally monitored by an individual within the company's leadership, designated as a "data protection officer."[116] This position is akin to a state's CIO.[117] A data protection officer would monitor compliance and develop training programs for employees in order to ensure continual compliance with the

112. McGeveran, *supra* note 8, at 1183.

113. Schwartz & Janger, *supra* note 12, at 954 n.188 (quoting BRUCE SCHNEIER, SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD xii (Carol Long ed., 2000)) (internal quotation marks omitted).

114. McGeveran, *supra* note 8, at 1183; *see also* Schwartz & Janger, *supra* note 12, at 954 (outlining the elements of "a reasonable program for data security").

115. McGeveran, *supra* note 8, at 1184.

116. *Id.* at 1185–87 (analogizing the position to the one required under the EU's General Protection Regulation); *see also* Schwartz & Janger, *supra* note 12, at 930 (stating that companies are often required to designate employees responsible for the companies data security practices) (citing Interagency Guidance Establishing Information Security Standards, 12 C.F.R. pt. 30 app. B, at 607 (2019)).

117. *See supra* INTRODUCTION. States implement reasonable data security standards for their governmental entities by creating a CIO. The CIO is responsible for overseeing state agencies' data security standards to ensure the security of the states' information systems.

protocol. Finally, the cycle comes back around to the start—auditing the process and its impact on the risks found in the initial assessments. This results in the start of another process for old, and in some instances, new risks associated with the company's data security policies.[118]

This self-policing method, or delegated regulation, inherent in a reasonableness standard, still comports with states' laws that seek to protect consumers' economic interests, while also seeking to control the cost of compliance for businesses.[119]

A. North Carolina's Statutory Focus on Consumers' Economic Interests

Applying a reasonableness standard on businesses' data security practices would allow North Carolina to maintain current consumer statutory protections in two ways. First, the proposed standard would be applied to personal information, which does not change the existing definition.[120] This would mean the consumers' economic interests at the heart of the breach notification statute remains the same—strictly protecting information that could be used to gain access to a consumer's financial resources. Second, in only allowing a private right of action for individuals "injured as a result of the violation,"[121] the proposed law would limit the claims that could be brought against a business who suffered a breach to only plaintiffs that experience injuries as a result of the business not adhering to the standards prescribed by law.[122]

Many times, state-specific data breach and consumer protections laws provide for regulator enforcement and a private right of action.[123] By

118. McGeveran, *supra* note 8, at 1187 (describing the similarities of such a system to existing federal regulations, such as HIPAA and FTC settlement agreements). McGeveran also discusses the three architecture requirements of an effective data security system: access controls, encryption, and multifactor authentication. *Id.* at 1188–93.

119. *See generally* Schwartz and Janger, *supra* note 12, at 926–27 (addressing regulatory forces guiding businesses to enhance their data security practices).

120. *See supra* Part I.A.2 (addressing the statutory definition of "personal information").

121. N.C. GEN. STAT. § 75-65(i) (2017).

122. There is another issue of standing, specifically the injury-in-fact requirement, in data breach lawsuits. That is a particularly contentious topic on which circuit courts are split, and it is beyond the scope of this Comment. *See generally* Nicholas Ronaldson, *Hacking: The Naked Age Cybercrime,* Clapper *& Standing, and the Debate Between State and Federal Data Breach Notification Laws*, 16 NW. J. TECH. & INTELL. PROP. 305, 314–20 (2019) (addressing the issue of standing under *Clapper v. Amnesty Int'l U.S.A.*, 568 U.S. 398 (2013), and *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015)); *see also* Priscilla Fasoro & Lauren Wiseman, *Standing Issues in Data Breach Litigation: An Overview*, INSIDE PRIVACY (Dec. 7, 2018), https://perma.cc/B9HS-AMS8.

123. In North Carolina, a violation of the statute is considered a violation of the state's UDTP, which allows the North Carolina Attorney General to bring an action against the

allowing both enforcement mechanisms, a state can ensure a business is not only complying with the requirements through regulator orders and settlements, but also strengthen consumer protections by providing a legal remedy to address the consumers' suffered harm.

As discussed in Part I, the proposed law would extend the existing law by incentivizing businesses' compliance with the reasonable security measures component. As currently structured, the law would create a punitive measure for non-compliant businesses whose consumers are actually injured by the business's non-compliance in the form of treble damages.[124] Incorporating a reasonableness standard in the statutes and making it a UDTP violation would provide an incentive for businesses to develop these measures, as to avoid possible violations. Such an extension could seamlessly ensure consumers' economic interest are well protected.[125]

B. A Reasonableness Standard in North Carolina

Part I established that North Carolina is weary of burdening businesses with the cost of data security.[126] Given this reality, this Section analyzes whether legislation is likely to pass or whether the costs might be too high. A business's goal is to turn a profit, and ideally increase that profit from one year to the next. To do that, many businesses will typically "grow in size to take on new tasks that are profitable for them, or else simply make contracts with others."[127] In terms of data security, businesses base their level of security on the costs associated with their legal liability and financial risk from a breach.[128] In other words, the benefits of having a robust data security program must outweigh the costs of implementing such a program.

---

violating organization as well as granting a private right of action to consumers who are actually harmed. N.C. GEN. STAT. § 75-65(i). This is also the case in Maryland and Tennessee. *See* MD. CODE ANN., COM. LAW § 13-401(e)(1) (LexisNexis through 2019); TENN. CODE ANN. § 47-18-2107(h) (2013).

124. N.C. GEN. STAT. § 75-65(f) (referencing N.C. GEN. STAT. § 75-1.1 (North Carolina's UDTP statute)).

125. The state legislature could always incorporate a certificate of merit requirement for any cause of action pertaining to the reasonable measures standard section of the statute; that could ensure businesses would not be burdened by the cost of potential frivolous litigation resulting from the adoption of this additional statutory requirement.

126. *See supra* Part I.B.

127. Schwartz & Janger, *supra* note 12, at 927 (describing the economic forces guiding businesses to invest in data security).

128. *Id.*

In 2019, "[i]t is not a question of if [a business] will suffer a data breach; it is a question of when."[129] The probability of a business experiencing a data breach in the next two years is 29.6 percent, up 31 percent since 2014.[130] A business's average cost of dealing with a data breach in the United States is $242 per record.[131] This year, the United States' average total cost of a data breach was $8.19 million, an increase of 130 percent over the past fourteen years.[132] Much of these costs come from the reputational harms associated with a breach, resulting in loss of customers, and the cost impact to an organization can last for years after the incident.[133]

These costs will likely continue to follow an upward trend,[134] forcing businesses to reevaluate their practices—or lack thereof—to minimize the cost burden associated with a breach. For businesses, it is a question of whether they want to pay now or later, in an environment where the costs associated with data breaches are increasing, while the costs of compliance with similarly-situated measures are becoming harder to avoid.

On the other hand, critics of privacy regulations have noted that the costs of compliance do not outweigh the benefits to the consumers.[135] In a recent survey of 250 California firms preparing for compliance with the state's new privacy rights legislation, 71 percent of survey respondents expected to spend at least six figures in related compliance expenses and 19 percent expected to spend over $1 million.[136] Some analysts have estimated the total businesses' cost of upfront compliance with the CCPA at $24.5

129. David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 936 (2016) (referring to cybersecurity experts' regular warning to businesses).

130. PONEMON INST., *supra* note 5, at 10.

131. *Id.* at 22.

132. *Id.* at 16.

133. The 2019 Ponemon Institute's study found that the average cost of lost business for breached entities was $1.42 million, and the breaches caused abnormal turnover of 3.9%. *Id.* at 5. Additionally, the study found that while 67% of the costs associated with a breach occurred in the first year, 22% accrued in the second year, and 11% of costs occurred more than two years after an incident. *Id.*

134. Additionally, these points do not include the costs of possible litigation and/or civil penalties associated with not complying with existing state statutes, which would only add to the costs associated with a breach.

135. *See* Roslyn Layton, *The Costs of California's Online Privacy Rules Far Exceed the Benefits*, AM. ENTERPRISE INST.: AEIDEAS (Mar. 22, 2019), (on file with Campbell Law Review) (citing TRUSTARC, CCPA AND GDPR COMPLIANCE REPORT: RESEARCH INTO U.S. COMPLIANCE STATUS AND PLANS FOR CALIFORNIA CONSUMER PRIVACY ACT AND EU GENERAL DATA PROTECTION REGULATION (2019)).

136. *Id.*

billion (this includes lost advertising revenue).[137] Other studies have found that federal legislation, similar to the GDPR, would result in an approximate loss of $122 billion to the U.S. economy in order for businesses to be in compliance with similar regulations.[138] As compared to compliance with more expansive regulations, like the CCPA, the implementation of a reasonable standard would involve a lower cost to the business.

Moreover, implementing reasonable security procedures actually has a mitigating effect on costs associated with a data breach. Taking measures like forming an incident response ("IR") team, conducting audits of the IR team's plan, and the extensive use of encryption have decreased the cost by $39.50 per record.[139] Just the formation of an IR team reduced the average total costs associated with a breach by as much as $360,000.[140]

Within this cost issue, many neglect the overlap in U.S. state-specific compliance costs and the GDPR and CCPA compliance costs.[141] Many companies that operate in the E.U. could find it cost effective to extend those GDPR-compliant services to U.S. citizens, likely at a marginal cost.[142] For example, the GDPR requires businesses that control or process data to have Data Protection Officers within their organization's leadership.[143] This is analogous to the "leadership" component of the "reasonable security procedures" cycle discussed in the previous Section. A U.S.-based company dealing with E.U. citizens' data is required to have data protection officers. Such a requirement would be an acceptable form of compliance under a state-adopted reasonable measures standard; therefore, the business's compliance with the GDPR would place them in compliance with the state-specific law.[144] Additionally, with the increasing number of states

137. *Id.*

138. Alan McQuinn & Daniel Castro, *The Costs of an Unnecessarily Stringent Federal Data Privacy Law*, INFO. TECH. & INNOVATION FOUND. (Aug. 5, 2019), https://perma.cc/WM4K-X5W9.

139. *See* PONEMON INST., *supra* note 5, at 38.

140. *Id.* at 37.

141. *See* Yaki Faitelson, *Yes, The GDPR Will Affect Your U.S.-Based Business*, FORBES (Dec. 4, 2017), https://perma.cc/7Z7T-RCW6.

142. Readers probably have already noticed the abundant amount of "cookie consent banners" that pop-up when visiting websites. This is another example of GDPR-compliant activity that businesses find cost-effective to apply across all platforms, not just in E.U. markets. *See Cookie Consent Banner-What Is It and How Do I Make It GDPR Compliant?*, COOKIEBOT, https://perma.cc/JNP7-XV8F.

143. *GDPR Key Changes*, *supra* note 142.

144. Another example of this type of cost-overlap would be when the GDPR first went into effect, Microsoft committed to extending the GDPR privacy protections to U.S. consumers. *See* Julie Brill, *Microsoft's Commitment to GDPR, Privacy and Putting Customers*

adopting such measures, businesses' compliance costs would overlap, likely reducing that burden.[145]

In a state that tends to avoid placing additional costs on businesses, these overlapping costs coupled with mitigation advantages could provide a low-budget transition to requiring a statutory reasonableness standard.

CONCLUSION

While state laws aim to protect consumers' financial interests, they oftentimes weigh in support of minimizing the costs of compliance for businesses; all the while risking the consumers' interests the statutes seek to protect in the first place. These types of statutory structures create little incentive for businesses to evolve in their data security practices. Businesses will continue to experience data breaches, and they will suffer from the increasing costs associated with those breaches; however, whether these costs outweigh the benefits offered by increased protections is a point of political contention. In this age of technological advancement, state legislatures are forced to balance these interests. Legislatures run the risk of weak consumer protections or restrictive regulations that stifle innovative enterprise. However, the adoption of a reasonableness standard for businesses' data security procedures could satisfy both of these sought-after interests.

This "reasonable" standard would be created and implemented by businesses to satisfy industry-specific needs in data security, providing businesses with flexibility while strengthening consumers' interests in protecting their personal information from misuse. The cost of compliance with that standard is not only dependent on the measures the industry suggests businesses take, but can actually mitigate the potential harms—and costs—associated with a breach. This standard supports the pro-business policies underlying many state statutes and provides consumers with the increased protections they want and need. In the current environment, where costs associated with data breaches are increasing while costs of

---

in Control of Their Own Data, MICROSOFT: MICROSOFT ON ISSUES (May 21, 2018), https://perma.cc/B9UM-5W4P.

145. For many businesses, this is the primary reason to support federal preemption in this area; however, states are in the best position to regulate data breaches affecting their residents' personal information. That argument is out of the scope of this Comment. *See* Needles, *supra* note 12; *see also* Ronaldson, *supra* note 122, at 317–19 (discussing the reasons state-specific breach notification laws are more efficient to protect consumers' interests than a federal law that would preempt state-based protections); *Federal Data Breach Legislation Should Not Preempt States*, NAT'L ASS'N ATTORNEYS GEN. (July 7, 2015), https://perma.cc/6KSY-W9UF.

compliance with similarly-situated measures are becoming harder to avoid, the question for businesses is whether they want to pay now or later.

James H. Ferguson III[*]

[*]J.D. Candidate 2021, Campbell University School of Law. The author would like to thank his wife, Kelsie, for her constant love and support; Professor Lucas Osborn, for his editorial support in the drafting of this comment; Ms. Phyllis Pickett, principal staff attorney for the North Carolina General Assembly's Bill Drafting Division, for assigning him the project that was the foundation for this comment; and the entire editorial team of the *Campbell Law Review*—especially "Spading Team Black," for source-pulling all of those state statutes.