University of Cincinnati Law Review

Volume 87 | Issue 4 Article 10

May 2019

The Ohio Data Protection Act: An Analysis of the Ohio Cybersecurity Safe Harbor

Daniel Shinkle
shinkldi@mail.uc.edu

Follow this and additional works at: https://scholarship.law.uc.edu/uclr

Recommended Citation
Daniel Shinkle, *The Ohio Data Protection Act: An Analysis of the Ohio Cybersecurity Safe Harbor*, 87 U. Cin. L. Rev. 1213 (2019)
Available at: https://scholarship.law.uc.edu/uclr/vol87/iss4/10

This Article is brought to you for free and open access by University of Cincinnati College of Law Scholarship and Publications. It has been accepted for inclusion in University of Cincinnati Law Review by an authorized editor of University of Cincinnati College of Law Scholarship and Publications. For more information, please contact ronald.jones@uc.edu.

THE OHIO DATA PROTECTION ACT: AN ANALYSIS OF THE OHIO CYBERSECURITY SAFE HARBOR

Daniel Shinkle

I. INTRODUCTION

The Ohio Data Protection Act ("Act"), formerly known as Senate Bill 220, was signed into law by Governor John Kasich on August 3, 2018.[1] The Act utilizes an innovative approach by allowing covered entities to take advantage of an affirmative defense for tortious claims following a data breach if the entity can demonstrate compliance with certain enumerated data protection frameworks.[2] The Act went into effect on November 2, 2018.[3] This Comment explores the policy implications of the Act and argues that it will be effective on two fronts. First, the Act will benefit the entities it covers by refusing to set a minimum standard of care and by employing a scalable approach. Second, the Act will protect Ohio consumer data by incentivizing covered entities to adopt relevant cybersecurity measures and by not completely barring consumer access to litigation.

This Comment's Background discusses the commonality of data breaches in the United States and how these data breaches frequently result in significant litigation. Then, the Background describes the United States legislative framework in reference to data security laws. Lastly, the background section discusses the specific provisions of the Ohio Data Protection Act and the data security approaches utilized by Colorado, Oregon, and New York.

Next, this Comment will focus on why the Ohio Data Protection law will be beneficial for both the covered entities it applies to and Ohio consumers. The Comment first explains that the Act will be beneficial for covered entities because it does not set a standard minimum care and utilizes a flexible approach. Then, the Comment contends that the Act will be beneficial for Ohio consumers because it will incentivize covered entities to protect their data and will not bar them from litigation. Lastly, this Comment discusses the effect that the Act may have on other states looking to implement cybersecurity legislation and the federal legislative landscape.

---

1. Jennifer Orr Mitchell & Jared M. Bruce, *Ohio Enacts First of Its Kind Data Protection Act*, LEXOLOGY, (Sept. 20, 2018), https://www.lexology.com/library/detail.aspx?g=d7a9e624-c57d-4916-8bc7-90bcc5cadb31.

2. *Id.*

3. *Id.*

Published by University of Cincinnati College of Law Scholarship and Publications, 2019

University of Cincinnati Law Review, Vol. 87, Iss. 4 [2019], Art. 10

II. BACKGROUND

Throughout the United States, the legislation and regulations put in place to counteract data breach and cybersecurity incidents are constantly developing and changing. First, this section underscores the significant risks data breaches pose for both entities that conduct business utilizing others' personal information and the individuals themselves by discussing recent data breach litigation. Next, this section considers the patchwork statutory and regulatory landscape that addresses liability allocation and the responsibilities private information holders possess. Lastly, this section describes pertinent data security laws implemented by various states, including the Ohio Data Protection Act, which will be the focus of the following discussion section.

A. Recent Data Breach Litigation and Settlements

Data breaches and cybersecurity compliance are among the most significant issues businesses must take into consideration when handling consumer information.[4] A data breach occurs when an individual gains unauthorized access to confidential information.[5] The information that people place online, including their names, telephone numbers, social security numbers, home addresses, email addresses, and credit card numbers, is at risk when a data breach occurs.[6] The unauthorized possession of this personal information may result in financial harm, identity theft, loss of privacy, or damaged reputation.[7] Further, data breaches are exceptionally challenging to prevent because of the numerous ways they can occur.[8] For instance, an individual may physically access a company's system by infiltrating the office or by using cyber prowess to circumvent implemented security networks and steal private information remotely.[9] Additionally, data breach and cybersecurity problems are prevalent across a wide swath of consumers and industries. Since January 2017, popular businesses such as Macy's,

4. Dennis Green & Mary Hanbury, *If You Shopped at These 16 Stores in the Past Year, Your Data Might Have Been Stolen*, BUSINESS INSIDER (Aug. 22, 2018, 5:49 PM), https://www.businessinsider.com/data-breaches-2018-4.

5. *Data Breach Lawsuit*, CLASSACTION.COM (July 2, 2018), https://www.classaction.com/data-breach/lawsuit/.

6. *Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes*, TREND MICRO (Aug. 10, 2018), https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101.

7. *Data Breach Lawsuit*, *supra* note 5.

8. *Cybersecurity Overview*, DEPARTMENT OF HOMELAND SECURITY (Sept. 27, 2016), https://www.dhs.gov/cybersecurity-overview.

9. *Data Breaches 101: How They Happen, What Gets Stolen, and Where it All Goes*, *supra* note 6.

Sears, Delta, Cheddar's, and Whole Foods, in addition to many others, have faced data breach issues.[10] The prevalence of these issues call into question the strategies companies are utilizing to protect compiled consumer data and the response society as a whole is implementing to address these problems.[11] The litigation involving these issues has brought cybersecurity concerns to the forefront of the legal, regulatory, and legislative communities' discussions.

Individuals or entities whose private information has been affected by a data breach often turn to litigation to hold companies liable for conduct that places their privacy and financial well-being at risk.[12] Many of these data breach lawsuits have resulted in massive settlements between businesses and consumers. For instance, in August 2018, a federal district judge in California approved a $115 million settlement involving allegations that Anthem had exposed sensitive information pertaining to 78.8 million customers.[13] Despite "[d]ata-breach litigation being in its infancy with threshold issues still playing out," the court found that the settlement was fair, adequate, and reasonable.[14] Furthermore, the court acknowledged that regardless of the settlement, it was not a foregone conclusion that Anthem's security measures were inadequate given that Anthem's security program had previously received praise within the industry.[15] Nevertheless, the settlement included funding for two years of credit monitoring for the plaintiffs but Anthem refused to admit any wrongdoing in the handling of personal data.[16]

There have been many other instances that emphasize the scope and magnitude of the potential harm data breach and cybersecurity issues create. In August 2013, every single user account linked to Yahoo was affected in an immense consumer data breach.[17] This instance involved

10. Dennis Green & Mary Hanbury, *supra* note 4.

11. *Id.*

12. *Data Breach Litigation*, LOCKRIDGE GRINDAL NAUEN P.L.L.P (last visited Sept. 27, 2018), https://www.locklaw.com/data-breach-litigation/.

13. Daniel Stoller, *Class Appeals Anthem Data Breach Settlement to Ninth Circuit*, BLOOMBERG LAW (Sept. 14, 2018), https://www.bloomberglaw.com/document/X4OR3U3K000000?bna_news_filter=privacy-and-data-security&jcsearch=BNA%252000000165d848d549ad7ffe5e846d0002#jcite.

14. In re Anthem, Inc. Data Breach Litig., 2018 U.S. Dist. Lexis 139271, **99 (N.D. Cal. 2018); *see generally* Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, 92 Notre Dame L. Rev. 1323 (2017) (discussing the split in federal courts regarding whether plaintiffs in data breach cases meet Article III standing requirements for injury and causation).

15. In re. Anthem, Inc. Data Breach Litig., at 2018 U.S. Dis. Lexis 139271 at **99.

16. Brendan Pierson, *Anthem to Pay Record $115 Million to Settle U.S. Lawsuits Over Data Breach*, REUTERS (June 23, 2017), https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML.

17. Selena Larsen, *Every Single Yahoo Account was Hacked – 3 Billion in All*, CNN (Oct. 4,

three billion user accounts and is the largest known breach of a company's network.[18] Then, in a separate incident the next year, 500 million more Yahoo accounts were affected when names, birth dates, and passwords were accessed.[19] Additionally, a third incident occurred in 2015 and 2016, when forged cookies were used to access users' accounts.[20] Litigation involving all three data breaches has been consolidated into a class action suit.[21] In March, 2018, a Northern District of California court granted in part and denied in part Yahoo's motion to dismiss.[22] Significantly, the judge denied Yahoo's motion to dismiss for claims arising out of tort and contract including negligence, breach of contract, breach of implied contract, and breach of implied covenant of good faith and fair dealing.[23]

Another recent and serious data breach involved the credit reporting firm Equifax.[24] The data breach affected 145.5 million Americans, almost half of the American population.[25] According to Equifax's 2017 Annual Report, Equifax is facing hundreds of class actions filed in state and federal courts where consumers are alleging a variety of common law and statutory claims.[26] Since then, the federal class action suits have been consolidated in the Northern District Court of Georgia for centralized proceedings.[27] Additionally, Equifax has pledged to continue cooperation with numerous city, state, and federal governmental agencies and regulatory bodies as the investigation continues.[28] Currently, no resolution to this massive litigation has been reached, but it clearly demonstrates the weight cybersecurity issues carry.

2017, 6:36 AM), https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html.

18. Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, THE NEW YORK TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

19. *Id.*

20. In re Yahoo! Customer Data Sec. Breach Litig., 313 F.Supp.3d 1113, 1123 (N.D. Cal. 2018).

21. *Id.* at 1126.

22. *Id.* at 1150.

23. *Id.* at 1131-39.

24. Hayley Tsukayama, *Equifax Faces Hundreds of Class-Action Lawsuits and an SEC Subpoena Over the Way it Handled its Data Breach*, THE WASHINGTON POST (Nov. 9, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/11/09/equifax-faces-hundreds-of-class-action-lawsuits-and-an-sec-subpoena-over-the-way-it-handled-its-data-breach/?utm_term=.3dcc2016b294.

25. Peter Blumberg, *How Much will Equifax Pay?*, BLOOMBERG BUSINESSWEEK (Nov. 14, 2017, 5:01 AM), https://www.bloomberg.com/news/articles/2017-11-14/how-much-will-equifax-pay.

26. Equifax, *2017 Annual Report*, 25 (2017).

27. *Id.*

28. *Id.*

B. Overview: United States Cybersecurity Legislative Framework

Chinese President Xi Jinping has stated, "Without cybersecurity, there is no national security."[29] Accordingly, last summer, China implemented a new cybersecurity law that provides the government with more power to monitor the abundant risks associated with cybersecurity threats despite an outcry of protests from private sector entities.[30] Contrary to the Chinese approach that emphasizes centralized national legislation, the United States' cybersecurity legislative and regulatory structure is much less uniform. While more than fifty federal statutes involve cybersecurity, there is no consistent federal framework in place.[31] Also, these different federal statutes tend to address cybersecurity by prescribing standards on an industry specific basis.[32] Thus, there is no broad national law that lays out uniform expectations in terms of protecting data and privacy across all sectors and industries.[33] While there is little federal law emphasizing data breaches and cybersecurity, an abundance of state legislation and regulations have been implemented that address these issues in a piecemeal, patchwork fashion with differing approaches and methodologies. Of the existing state cybersecurity statutes, the Ohio Data Protection Act demonstrates a unique and novel approach to addressing the significant harm caused by data breaches by shaping the applicable frameworks a covered entity may follow and by providing incentive for an applicable entity to do so.

C. The Ohio Data Protection Act

Put simply, Ohio's new cybersecurity law is meant to incentivize entities to be proactive when handling consumer data by complying with certain enumerated frameworks.[34] The bill aims to achieve this goal by providing a safe harbor for companies that comply with its frameworks, suffer a data breach, and are later sued in tort by allowing for an affirmative defense.[35] The legislation clearly dictates that the provision

29. Samm Sacks, *China's Cybersecurity Law Takes Effect: What to Expect*, LAWFARE (June 1, 2017, 10:57 AM), https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

30. Jyh-An Lee, *Hacking Into China's Cybersecurity Law*, 53 Wake Forest L. Rev. 57, 58-60 (2018).

31. Eric Fisher, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, CONGRESSIONAL RESEARCH SERVICE, 2 (Dec. 12, 2014).

32. Michael Volkov, *Cybersecurity: The Law and Regulatory Framework*, VOLKOV (Jan. 25, 2018), https://blog.volkovlaw.com/2018/01/cybersecurity-law-regulatory-framework/.

33. JEFF KOSSEFF, CYBERSECURITY LAW 1 (Wiley, 2017).

34. *Client Alert: Ohio Enacts Cybersecurity Safe Harbor Law for Data Breach Litigation*, VORYS, SATER, SEYMOUR, AND PEASE LLP, (Aug. 6, 2018), https://www.vorys.com/publications-2241.html.

35. *Final Analysis: Sub. S.B. 220*, Ohio Legislative Service Commission, 1 (2018),

does not promulgate a new set of minimum standards for entities to meet in relation to cybersecurity and data protection.[36] Rather, it is merely meant to entice applicable entities to adopt stronger data protection methods by offering an attainable affirmative defense. Additionally, the provision expressly indicates that it does not create a private right of action.[37] It is not intended to allow individuals to sue certain entities for not meeting the requirements it enumerates. Regardless, while the Data Protection Act employs a broad application, the safe harbor does not automatically apply following a data breach. There are several requirements that must be fulfilled before an entity may take advantage of the affirmative defense.

i. Definitional Applicability

First, in order for the safe harbor to apply, the business asserting the affirmative defense must be a "covered entity".[38] Under the statute, a "covered entity" includes a business that "accesses, maintains, communicates, or processes personal information or restricted information in or through one or more systems, networks, or services located in or out of this state."[39] The statute then defines a "business" loosely as any type of entity, whether operating for profit or not, and including financial institutions.[40] Further, the information the covered entity possesses must also be classified as either personal or restricted information.[41] The statute defines "personal information" by referencing a previous section of the Ohio Revised Code that states personal information includes an individual's name that is linked to one or more of the following: social security number; driver's license number; an account number; or a credit card number.[42] However, "restricted information" is defined within the statute in broader terms. "Restricted information" relates to information, other than personal information, that can be traced or linked to an individual when combined with other information, including personal information, or alone.[43] Thus, even before the affirmative defense is asserted, the entity must meet these definitional requirements in order to ensure applicability.

---

https://www.legislature.ohio.gov/download?key=10218&format=pdf.

36. *Id.* at 2.

37. OHIO REV. CODE ANN. § 1354.04 (LexisNexis 2018).

38. *Id.* § 1354.02(A).

39. *Id.* § 1354.01(B).

40. *Id.* § 1354.01(A).

41. *Id.* § 1354.02(A).

42. *Id.* § 1349.19(A)(7)(a)(i-iii).

43. *Id.* § 1354.01(E).

ii. Ohio Data Protection Act Cybersecurity Measures

The most significant portion of the Ohio Data Protection Act involves the frameworks covered entities must conform with to receive safe harbor protection. First, covered entities must create written cybersecurity programs that describe the methods the entity will employ and follow to protect personal or restricted information.[44] Further, the program must include "administrative, technical, and physical safeguards," and conform to "industry recognized cybersecurity framework[s]," which are described in the next section of the statute.[45] Additionally, besides implementing a cybersecurity program and adhering to it, the statute provides two additional considerations that must be accounted for when deciding the coverage of the safe harbor. First, the provision indicates that the cybersecurity plan must be designed to protect data and prevent threats.[46] Second, the program must be an appropriate scale and scope when evaluating several different factors involving the entity's characteristics and its business operations, the confidentiality of the information the entity has obtained, the costs of implementing a cybersecurity program, and the resources available to the entity.[47] Nevertheless, the question remains what constitutes a covered entity's conformity to industry recognized cybersecurity frameworks.

The next statutory section answers the conformity concern by putting forth three ways an entity may establish a cybersecurity program that is reasonably compliant within industry recognized cybersecurity frameworks.[48] The first way provides several different standards that covered entities may choose as a basis to reasonably comply.[49] The first three standards that covered entities may evaluate involve standards promulgated by the National Institute of Standards and Technology (NIST).[50] The NIST is a subset of the United States Department of Commerce that provides technology, measurement, and standards to maximize efficiency in the United States' economy.[51] Part of NIST's

44. *Id.* § 1354.02(A).

45. *Id.*

46. *Id.* § 1354.02(B); A covered entity's cybersecurity program shall be designed to do all of the following with respect to the information described in division (A)(1) or (2) of this section as applicable: (1) Protect the security and confidentiality of the information; (2) Protect against any anticipated threats or hazards to the security or integrity of the information; (3)Protect against any unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

47. *Id.* § 1354.02(C)(1-5).

48. *Id.* § 1354.03.

49. *Id.* § 1354.03(A).

50. *Id.* § 1354.03(A)(1)(a-c).

51. *About NIST,* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (last visited Sep. 27,

function involves establishing cybersecurity standards that are cost effective and promote the efficiency and well-being of the American economy.[52] Next, other standards set forth by additional cybersecurity authorities including FedRAMP, the Center for Internet Security, and the International Organization for Standardization are recognized as additional industry recognized cybersecurity frameworks.[53] Thus, any covered entity that demonstrates reasonable compliance with the requirements of one of these standards employs an industry recognized cybersecurity framework.

Further, a covered entity may fulfill the industry recognized cybersecurity framework requirement if its program fulfills the Payment Card Industry (PCI) Data Security Standard in addition to one of the frameworks included above.[54] The entity must conform to the most current standard established within a year of the update's publication.[55] Similar to the NIST, the PCI Data Security Standard is meant to offer standards that implement stronger security practices as a means of protecting confidential information. The PCI standards focus on protecting cardholder data through a number of different technical and particularized strategies as opposed to the NIST standards that may have broader applicability.[56]

Lastly, a covered entity's program may qualify for safe harbor protection if the covered entity meets requirements included in several industry specific federal laws.[57] These federal laws include the Health Insurance Portability Act of 1996 (HIPPA), the Gramm-Leach-Bliley Act of 1999, the Federal Information Security Modernization Act of 2014, and the Health Information Technology for Economic and Clinical Health Act. Respectively, these federal laws relate to healthcare, financial institutions, federal agencies, and healthcare providers.[58] These laws are also indicative of the federal regulatory framework that addresses cybersecurity in a piecemeal basis as opposed to overarching legislation. Covered entities, however, that must already comply with these federal laws may be able to reap the benefits of the

2018), https://www.nist.gov/about-nist.

52. Ron Ross, Patrick Viscuso, Gary Guissanie, Kelley Dempsey, & Mark Riddle, *NIST Special Publication 800-171*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Page ii (2016), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

53. OHIO REV. CODE ANN. § 1354.03(A)(1)(d-f).

54. *Id.* § 1354.03(C)(1).

55. *Id.* § 1354.03(C)(2).

56. *Payment Card Industry Data Security Standard*, SECURITY STANDARDS COUNCIL, 5 (2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1542496050158.

57. OHIO REV. CODE ANN. § 1354.03(B).

58. *Final Analysis: Sub S.B. 220*, *supra* note 35 at 7.

safe harbor provision, as long as their programs are current.

When a cybersecurity framework is amended, or a federal statutory framework is updated, the covered entity has one year to modify its plan to reasonably conform with the update to qualify for the affirmative defense.[59] Additionally, if a covered entity reasonably conforms to a combination of frameworks or standards, and two or more of the frameworks are revised, the entity must conform to all of the applicable, revised frameworks within a year of the revisions.[60] Thus, the Ohio statute clearly identifies the industry recognized cybersecurity frameworks that covered entities must fulfill in order to receive protection in the event they are sued in tort for failing to protect private or restricted information.

D. Alternative State Cybersecurity Strategies

Other states take different approaches involving cybersecurity legislation that address the requirements entities who accumulate others' private information must follow. This subsection discusses various strategies that other states employ to combat cybersecurity issues by examining the approaches of Colorado, Oregon, and New York. While almost all states have laws relating to the disclosure of data breaches, fewer states have legislation that deal explicitly with data security.[61] Because this Comment focuses on the Ohio Data Protection Act, this subsection will discuss alternative strategies regarding data security legislation or regulation while keeping in mind that almost all states require disclosure of data breaches that may have an adverse effect on individuals to whom the information relates.

i. Colorado Data Security Law

Similar to Ohio, Colorado recently enacted a significant cybersecurity law that includes data security provisions. The Colorado legislation, which went into effect on September 1, 2018, contains key differences from the Ohio legislation, though enacted in a similar timeframe.[62] First, the Colorado legislation, which applies to persons who maintain, own, or license "personal identifying information" of an individual residing in Colorado, lays out a broad definition of "personal identifying

59. *Id.* at 7- 8.

60. OHIO REV. CODE ANN. § 1354.03(D).

61. Jeff Kosseff, *supra* note 33 at 36, 42.

62. *What to Know About New Colo. Data Privacy Law*, LAW 360 (June 14, 2018), https://advance.lexis.com/api/permalink/5965c00d-cb8f-4ed6-ac85-4909c19e0082/?context=1000516.

information."[63] In addition to the more common terms identified under Ohio law, Colorado's definition of "personal identifying information" in the data security context includes: passport numbers; biometric data; and employer, student, or military identification numbers.[64] Second, Colorado's requirements and obligations placed on covered entities is very different from Ohio. Under the statute, covered entities must maintain "reasonable security procedures and practices that are appropriate to the personal identifying information and the size of the business and its operations."[65] The Colorado statute does not offer much additional insight into which practices are considered reasonable from a compliance perspective besides acknowledging that entities in compliance with applicable state or federal "laws, rules, regulations, guidances, or guidelines" meet this section's requirements.[66] Third, the law extends similar obligations to covered entities that utilize third-party service providers to ensure that personal identifying information is not at risk while in the third-party's hands.[67] Thus, even though the obligations established by Colorado Data Security Law appear much more interpretive, the obligations are mandatory for covered entities as a means of protecting personal identifying information.

ii. Oregon Information Security Law

While Colorado's statute employs a vague and flexible standard regarding the expectations of covered entities, Oregon utilizes specific requirements more analogous to the Ohio Data Security Act. First, Oregon's data security law applies to any individual who has control over, or access to, another's personal information.[68] Next, the statute calls on applicable entities to protect the personal information in possession and enumerates some specific ways that an entity may comply.[69] Similar to Ohio and Colorado's acknowledgement of federal data protection statutes, Oregon provides that an entity is compliant when applicable federal cybersecurity requirements, like HIPPA and the Gramm-Leach-Bliley Act, are fulfilled.[70] For other entities, the statute designates requirements for administrative, technical, and physical

63. COLO. REV. STAT. § 6-1-713(2)(b) (2018).
64. *Id.*
65. *Id.* § 6-1-713.5(1).
66. *Id.* § 6-1-713.5(4).
67. *Id.* § 6-1-713.5(2).
68. OR. REV. STAT. § 646A.622(1) (2018).
69. *Id.* § 646A.622(1-2).
70. *Id.* § 646A.622(2)(b-c).

safeguards.[71] The key difference between the Ohio Data Protection Act and the Oregon legislation in this regard is that the Ohio legislation defers specific framework requirements to other relevant authorities, while the Oregon statute explicitly designates methods for administering safeguards. For example, in reference to administrative safeguards, the statute requires entities to designate employees to coordinate the security program, identify and foresee risks, and assess whether the safeguards are adequate to guard against potential risks.[72] Thus, Oregon cybersecurity law maintains a very specific approach in terms of the expectations and burdens placed on covered entities and the requirements they must fulfill.

iii. New York Cybersecurity Requirements for Financial Service Companies

New York currently employs a regulatory approach to monitoring various entities' cybersecurity strategies, as opposed to the legislative approach utilized by Ohio, Colorado, and Oregon. The New York Department of Financial Services (DFS) regulates financial service institutions in New York to promote a strong financial sector.[73] DFS promulgated a cybersecurity regulation that applies specifically to any entity that is chartered, licensed, or approved to operate in New York State by DFS.[74] Thus, covered entities range from small brokers to international firms and include insurance companies, banks, money transmitters, and mortgage brokers.[75] The regulation is meant to combat the serious risks financial institutions face as significant targets of cybersecurity threats by taking a prescriptive, measured approach.[76] Enacted recently, the New York DFS regulations are among the first to regulate cybersecurity throughout an entire industry.[77] Because of the prominence of the financial sector in New York and its inherent cybersecurity risks, the New York regulations are expected to be significantly impactful on the internal functions of numerous financial

71. *Id.* § 646A.622(2)(d).

72. *Id.*

73. *23-NYCRR-500: DFS Cybersecurity Regulation*, NEW YORK DEPARTMENT OF FINANCIAL SERVICES, 2 (Dec. 6, 2017), https://www.treasury.gov/initiatives/fio/Documents/December2017FACI_NYDFS.pdf.

74. *Id.* at 6.

75. *Id.*

76. 23 NYCRR 500.00 (2018).

77. Barry Timkin and Kenneth Labbate, *New York Department of Financial Services Cybersecurity Regulations: An Update*, NEW YORK LAW JOURNAL (June 28, 2018), https://www.law.com/newyorklawjournal/2018/06/28/062918ny_temkin2/.

institutions.[78]

As opposed to the legislative methods discussed above, the New York DFS approach relating to financial institutions is much more comprehensive in terms of its requirements by setting forth seventeen regulations.[79] First, covered entities must implement "cybersecurity programs" that protect the covered entity's "information systems," which are defined as "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information[.]"[80] The "cybersecurity program" identifies and assesses risk; protects information systems and nonpublic information; detects, responds, and recovers from cybersecurity events; and fulfills applicable regulatory reporting obligations.[81] In these regulations, "nonpublic information" includes information relating to any individual that can be used to identify the individual in combination with a social security number, drivers' license number, account number, security code, or biometric records.[82] Additionally, each covered entity must implement an approved "cybersecurity policy" that addresses a number of different focus areas depending upon applicability.[83] The entity must also designate a "Chief Informational Security Officer" (CISO) to implement the cybersecurity program and develop a report to be reviewed internally on an annual basis.[84] The CISO's report may consider the entity's cybersecurity programs and policies and their effectiveness; the material risks that the entity may face; and any cybersecurity incidents that occurred during the relevant time period.[85]

There are many more regulations set forth by DFS that provide for additional requirements covered entities must meet. For instance, the regulations require each covered entity's program to include penetration testing and vulnerability assessments on a repeating basis.[86] Penetration testing involves attempting to circumvent the covered entity's security

78. *Id.*

79. *Id.*

80. 23 NYCRR 500.01(e).

81. 23 NYCRR 500.02(b).

82. 23 NYCRR 500.01(g)(2).

83. 23 NYCRR 500.03; A covered entity's cybersecurity policy must address the following areas if applicable: information security; data governance and classification; asset inventory and device management; access controls and identity management; business continuity and disaster recovery planning and resources; systems operations and availability concerns; systems and network security; systems and network monitoring; systems and application development and quality assurance; physical security and environmental controls; customer data privacy; vendor and Third Party Service Provider management; risk assessment; and incident response.

84. 23 NYCRR 500.04.

85. 23 NYCRR 500.04(b).

86. 23 NYCRR 500.05.

to test its strength.[87] Additionally, covered entities must "implement written policies and procedures to ensure the security of Information Systems and Nonpublic Information that are accessible, or held by, Third Party Service Providers."[88] Thus, covered entities must carry out due diligence on the third parties they conduct business with that have access to sensitive information and determine the adequacy of the third-parties' cybersecurity practices.[89] Also, covered entities must provide training to employees related to the cybersecurity risks the institution faces.[90] Lastly, the regulations implement other requirements relating to specific cybersecurity practices including access privileges, application security, multi-factor authentication, and encryption of nonpublic information.[91] Noncompliance with any of the DFS regulations may lead to fines or review of the relevant cybersecurity program.[92]

Additionally, it should be mentioned that the New York Attorney General introduced an act in the State's legislature that reaches beyond the financial sector.[93] The act, called Stop Hacks and Improve Electronic Data Security (SHIELD), is meant to apply to all companies who collect New York residents' information.[94] SHIELD would require companies to adopt reasonable safeguards as a means of protecting private information through compliance with enumerated requirements and with relevant federal or regulatory law.[95] Interestingly, companies could also demonstrate compliance by becoming certified annually by an authorized third-party assessor.[96] As of this time, however, SHIELD remains in committee in the New York Senate.[97] SHIELD demonstrates

87. 23 NYCRR 500.01(h).

88. 23 NYCRR 500.11(a).

89. *Id.*

90. 23 NYCRR 500.14.

91. 23 NYCRR 500.07; 500.08; 500.12; 500.15.

92. Jake Olcott, *5 Highlights of the NYDFS Cybersecurity Regulations*, BITSIGHT TECHNOLOGIES (Dec. 14, 2017), https://www.bitsighttech.com/blog/nydfs-cybersecurity.

93. Courtney Bowman, *A Primer on the SHIELD Act: New York's Move to Adopt More Stringent Data Security Requirements*, PROSKAUER ROSE LLP (Mar. 21, 2018), https://privacylaw.proskauer.com/2018/03/articles/cybersecurity/a-primer-on-the-shield-act-new-yorks-move-to-adopt-more-stringent-data-security-requirements/.

94. Courtney Bowman, *A Primer on the SHIELD Act: New York's Move to Adopt More Stringent Data Security Requirements*, PROSKAUER ROSE LLP (Mar. 9, 2018), https://www.mindingyourbusinesslitigation.com/2018/03/a-primer-on-the-shield-act-new-yorks-move-to-adopt-more-stringent-data-security-requirements/.

95. Courtney Bowman, *A Primer on the SHIELD Act: New York's Move to Adopt More Stringent Data Security Requirements*, PROSKAUER ROSE LLP (Mar. 12, 2018), https://www.mindingyourbusinesslitigation.com/2018/03/a-primer-on-the-shield-act-new-yorks-move-to-adopt-more-stringent-data-security-requirements-part-ii/.

96. *Id.*

97. THE NEW YORK STATE SENATE, (last visited Feb. 9, 2019), https://www.nysenate.gov/legislation/bills/2017/s6933.

the continuous shifting and development of the United States legislative cybersecurity framework.

III. DISCUSSION

The Ohio Data Protection Act was enacted to provide an affirmative defense for entities that handle sensitive information wrongly, allowing for unauthorized access. This section explains why the Ohio Data Protection Act will benefit covered businesses that handle consumer data and will also explain why the Act will be advantageous for Ohio consumers who entrust covered entities with their personal and private information. This section considers these topics by referencing the previously discussed laws and regulations that indicate the variety of methods employed to address data breaches by comparing them to the strategies used by the Ohio Data Protection Act.

A. The Ohio Data Protection Act Will Be Beneficial for Covered Entities

In January 2018, the Ohio Chamber of Commerce testified in support of then-Senate Bill 220 exulting its value for Ohio businesses and industry.[98] This testimony is indicative of the value that this legislation is perceived to have among the business community by providing an affirmative defense to those who demonstrate that they reasonably complied with industry standards in the face of a data breach. The Act will be beneficial for applicable businesses because it does not create a minimum standard of care and its structure emphasizes flexible cybersecurity approaches. This subsection demonstrates why the enactment of the Act is perceived to be positive by those in the business community by first discussing the significance of the Act's refusal to create a minimum standard of care. Next, this subsection will discuss the flexibility the Act utilizes in terms of scope and choice.

i. The Act Does Not Create a Minimum Standard of Care

First, the Ohio Data Protection Act is advantageous for businesses because of its refusal to create a minimum standard of care. The Act explicitly states that it does not intend to create a minimum cybersecurity standard that must be achieved by an entity, or impose liability on applicable entities whose practices are not in compliance.[99]

98. Don Boyd, *Ohio Chamber Supports Business Cybersecurity Safe Harbor*, OHIO CHAMBER OF COMMERCE (Jan. 11, 2018), http://allforohio.com/2018/01/11/ohio-chamber-supports-business-cybersecurity-safe-harbor/.

99. Ohio Substitute Senate Bill 220, § 3 (2018).

Rather, the Act intends to incentivize covered entities to comply with the standards it dictates in order to receive additional protection should a data breach occur. By providing a safe harbor for meeting certain standards, the Act is essentially promoting optional cybersecurity frameworks. If an entity chooses not to follow these frameworks, the provision cannot be used against them should they be sued in tort for mishandling personal information. Thus, it does not impose any additional requirements among businesses who handle personal information; it simply provides an incentive for adopting the enumerated cybersecurity frameworks.

The Act's approach is certainly different from the Colorado, Oregon, and New York legislation and regulations described above. Each of these states' cybersecurity measures mandate compliance with various stipulations, though the specificity and requirements themselves vary between the three states. By mandating methods regarding the handling of sensitive information, these states are imposing additional burdens on applicable entities that must be met. For instance, an individual who has access or control over an Oregon resident's personal information must either comply with applicable federal law or meet specified enumerated requirements relating to administrative, physical, and technical safeguards. If federal law applies, the hypothetical entity may already comply by meeting those requirements. The Oregon law, however, imposes new burdens on applicable entities outside the scope of federal cybersecurity legislation. Thus, the Oregon Information Security Law designates minimal standards that must be met in order to be compliant. The same can be said for covered entities under the Colorado Data Security Law and financial institutions affected by the requirements promulgated by the New York DFS.

Under the Colorado, Oregon, and New York statues that mandate requirements to be met by those handling sensitive personal information, a covered entity may not be absolved from liability if it meets mandatory standards and suffers a data breach that exposes information in its possession. For instance, in the Anthem litigation, the court approved a settlement between Anthem and the plaintiffs despite the approval that many experts bestowed upon Anthem's cybersecurity program and its response to the data breach.[100] While the court did acknowledge the uncertainty regarding novel questions the litigation posed, the litigation likely would have been resolved differently if the Ohio Data Protection Act had been applicable. If Ohio law had been applied to this suit, and the cause of action was in tort, an entity that maintains a reputable cybersecurity program would likely be able to

100. In Re. Anthem, Inc. Data Breach Litig., *supra* note 15.

assert the affirmative defense at the pleading stage by filing a motion to dismiss. Thus, the covered entity would have no need to settle if it is permitted to successfully assert the affirmative defense at the pleading stage and absolve itself of tortious liability, regardless of potential negligence.

Therefore, the Ohio Data Protection Act is very beneficial for businesses that can demonstrate compliance by not creating a minimum standard of care, but instead providing for incentive to implement data protection. However, the Act is also beneficial for businesses who choose not to comply, because it does not impose additional burdens or requirements. It simply disallows the application of the affirmative defense. Regardless, an entity who chooses not to follow the provision's standards may still be able to prevail through other means or arguments.

ii. The Act's Scope and Flexibility is Advantageous for Covered Entities

The Ohio Act is also advantageous for businesses because of the breadth of its scope and its flexible approach. First, the breadth of the entities covered by the Ohio Act is beneficial to a variety of businesses by allowing them the opportunity to take advantage of the safe harbor. The Act covers a wide swath of businesses or other organizations that access, maintain, communicate, or handle personal information. This broad applicability is different from the other examples examined in this Comment. For example, the New York regulations promulgated by DFS apply only to financial institutions.[101] The Ohio Act includes financial institutions but reaches farther by incorporating other types of entities in various industries. This inclusion means the Ohio Act is similar to the Oregon legislation, which is applicable to entities that handle or have access to another's personal information.[102] The Act, however, is notably different because it grants an expanded number of entities an opportunity to take advantage of the affirmative defense in place of requiring additional action. For instance, a small business in Ohio that handles Ohio citizens' personal information may choose to adopt the frameworks enumerated under the Ohio Act and receive protection if it suffers a data breach. Alternatively, if the Ohio business does not consider the risk to be substantial enough to warrant such investment, it may not adopt the frameworks and will assume the risk. Regardless, the decision remains with the business.

Additionally, the Ohio Act's flexibility is attractive for businesses because the entities' cybersecurity programs will be considered in a

101. 23 NYCRR 500.01(c).

102. OR. REV. STAT. § 646A.622(1), *supra* note 68.

measured and adjustable fashion through the application of certain factors. The Ohio Act considers: (1) the size and complexity of the entity; (2) the nature and scope of its activities; (3) the sensitivity of the relevant information; (4) the cost and availability of tools to improve security; (5) and the resources available to the entity when considering the appropriateness of an entity's cybersecurity program.[103] This provision allows for a measured approach that does not require entities who possess information that is less sensitive than others to over-invest in cybersecurity. Rather, the entities' compliance with the industry recognized cybersecurity considered will not be a bright line decision and will allow for interpretation of the specific facts in each situation where the affirmative defense is asserted. Furthermore, the Ohio Act only requires *reasonable compliance* with the industry recognized standards, as opposed to strict implementation.[104] Colorado adopts a similar approach by mandating "reasonable security procedures and practices that are appropriate to the personal identifying information and the size of the business and its operations."[105] Again, these approaches permit businesses to undertake cybersecurity measures that are appropriate for their specific circumstances in place of imposing oppressive and unnecessary cybersecurity standards for entities who may not need to erect such substantial defenses.

Lastly, the flexibility of the Ohio Data Protection Act will be advantageous for applicable entities by providing choices as to which industry recognized framework the covered entity would like to employ to receive safe harbor protection. The Act provides for a covered entity to select a cybersecurity program that reasonably conforms to an industry recognized cybersecurity framework and enumerates the various options.[106] These options permit the covered entity to formulate a cybersecurity program that is appropriate for its situation by not mandating a specific approach. While the industry recognized cybersecurity standards are long, tedious, and complex, the entity has the opportunity to choose one that is appropriate, and also take advantage of the flexibility built into the programs themselves. For instance, the NIST Framework for Improving Critical Infrastructure Cybersecurity acknowledges that it is not a one-size-fits-all approach and sets forth a wide variety of ways to use the framework that is left to the discretion of the covered entity.[107] Further, an entity looking to take

103. OHIO REV. CODE ANN. § 1354.02(C), *supra* note 47.

104. *Id*. § 1354.03(A), *supra* note 49.

105. COLO. REV. STAT. § 6-1-713.5(1), *supra* note 65.

106. OHIO REV. CODE ANN. § 1354.03(A), *supra* note 48.

107. *Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, VI (Apr. 16, 2018),

advantage of the safe harbor provision could select to reasonably comply with the Framework for Improving Critical Infrastructure Cybersecurity, or could decide to pursue another option. This flexibility allows for businesses to decide upon cybersecurity measures that are receptive to their specific situations.

Contrarily, the New York and Oregon approaches mandatorily limit the covered entities' cybersecurity programs and methodologies. While the New York regulations apply strictly to financial institutions, they do not permit the discretion for covered entities that the Ohio Act does. For instance, the New York regulations require the appointment of a Chief Information Security Officer, implementation of both a cybersecurity policy and program, and expectations involving many other specific requirements.[108] Similarly, Oregon requires covered entities to comply with certain safeguards.[109] These methods permit significantly less discretion than the Ohio Act on two levels. First, the Ohio Act itself is optional. Entities are not required to meet the industry recognized standards, but they are rewarded with an applicable safe harbor if they do. Second, the Ohio Act provides more options and choices, as opposed to setting requirements that mandate a covered entity's course of action. Therefore, the Ohio Act's structure which allows flexible choices will be beneficial for Ohio business by permitting them to pursue appropriate, scalable cybersecurity measures.

Thus, the Ohio Act will be beneficial for businesses that handle personal information by not creating a standard of care and allowing for a flexible approach. While this Act will be beneficial for the business community, the effect of the legislation on the consumers whose information is being handled must also be taken into consideration.

B. The Ohio Data Protection Act's Effect on Consumers

While the Ohio Data Protection Act will likely be beneficial for covered entities who handle sensitive information, the effect the Act will have on consumers and others who provide information to the covered entities is slightly more questionable. The Ohio Data Protection Act is unique in offering a carrot approach as opposed to the stick, but questions remain about the Act's effectiveness in terms of actually protecting consumer data and whether the Act will serve as a bar to litigation. Despite these concerns, the Ohio Data Protection Act will be effective in protecting sensitive information by incentivizing covered entities to adopt industry recognized frameworks. Additionally, the Act

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

108. 23 NYCRR 500.04, *supra* note 84.

109. OR. REV. STAT. § 646A.622, *supra* note 69.

will not serve as a bar to cybersecurity litigation in Ohio because the law only bars tortious claims and judges will be permitted to evaluate whether covered entities are actually complying with industry recognized frameworks. This section first discusses how effective the Act will be in protecting sensitive information and then will focus on whether the Act will bar litigants from seeking redress for harmful data breaches.

i. The Act Will Effectively Protect Consumer Data

The Ohio Data Protection Act is unique in offering an advantage to covered entities that meet enumerated standards. This approach, which offers an incentive for companies to develop their cybersecurity measures in compliance with industry recognized frameworks, is essential in achieving the law's purpose of protecting consumer data by making covered entities more likely to adopt cybersecurity measures that are useful, effective, and current. Unlike the Colorado, Oregon, and New York laws and regulations that set requirements for entities that handle private information, entities under the Ohio law gain an advantage by complying with its stipulations. This method sets a realistic and helpful benchmark for covered entities to reach as they formalize their cybersecurity measures and provides incentive to do so, which in turn, creates an environment that is beneficial for consumers that may not occur under the other approaches.

For instance, the New York regulation promulgated by DFS mandates that financial institutions meet a number of requirements that are intended to strengthen security of sensitive information in possession of applicable institutions.[110] While the numerous requirements placed on financial institutions are well intended to protect consumer data, what happens if an institution strictly adheres to all seventeen regulations, but still suffers a data breach that exposes various consumers to risk? Even if the institution addresses all of the areas of concern, it may very well face liability in the face of the data breach. Thus, in instances like this, covered institutions may pursue cybersecurity protections in a less vigorous or fervent manner. Regardless of the institution's compliance with the regulations, the frequency of data breaches and the costs of addressing these concerns may drive the institutions to pursue counteractive cybersecurity measures less fervently. This scenario presents a lose-lose situation for institutions that may result in consumer data being compromised. First, if institutions do not comply with the regulations implemented to protect data, they may face sanctions or

110. 23 NYCRR 500.00, *supra* note 76.

other penalties due to their noncompliance. Second, they may undertake the means to comply with the regulations and incur the costs, but then suffer a data breach and face additional costs through litigation or settlement. Thus, the stick method utilized by New York, Oregon, and Colorado may actually discourage companies and institutions to proactively protect consumer data.

Conversely, the carrot method that Ohio employs actually encourages covered entities to be proactive to protect consumer data. Instead of facing additional costs in the face of a data breach, an entity that can demonstrate compliance with industry recognized standards may be absolved from tortious liability.[111] Unlike the other methods described above, covered entities under the Ohio law will not face a lose-lose situation that may result in a reduction of vigor in implementing cybersecurity defense. Rather, covered entities will realize the value in implementing the industry recognized frameworks which will have the effect of reducing the aggregate risk of consumers who provide information to the various covered entities. Despite the fact that covered entities are not required to enact any sort of cybersecurity protection, companies will very likely see the value in complying with the enumerated frameworks given how prevalent data breaches are in today's environment. Thus, more entities and companies will apply these standards in order to capitalize on the reward and consumer data, as an aggregate, will be more secure.

Furthermore, the Ohio Data Protection Act will be beneficial for consumers because it encourages covered entities to adopt measures that are actually useful in terms of protecting consumer information. The methods that the Act encourages entities to adopt are "nationally and internationally recognized and proven."[112] Additionally, the methods enumerated in the Act are effective due to their scalability and sustainability.[113] Thus, the increased incentive that the Act creates by offering an affirmative defense to those who reasonably comply with the industry recognized frameworks, combined with the value of these frameworks as effective countermeasures to data breaches, ensures that Ohio consumer data will be more protected than before the Act was implemented.

Lastly, the Ohio Data Protection Act emphasizes protection of consumer data by requiring covered entities seeking the safe harbor's protection to keep their cybersecurity programs up to date. Specifically,

111. *Final Analysis: Sub. S.B. 220*, at 1, *supra* note 35.

112. Letter from Kirk Herath, VP, Chief Privacy Officer, Associate General Counsel, to the Honorable Louis W. Blessing III, Chairmen, House Government Accountability and Oversight Committee (June 26, 2018).

113. *Id.*

the Act requires covered entities comply with updates to industry recognized frameworks or federal laws within a year.[114] This requirement means that covered entities must be aware of changes of the industry recognized frameworks or applicable federal law, and must implement those changes to keep their cybersecurity measures up to date and effective. This acknowledgment of the continually adaptive cybersecurity landscape is another way the Ohio Act effectively incentivizes covered entities to responsibly handle consumer data. The other laws, like Colorado, that require applicable businesses and entities to carry out reasonable measures would also likely involve keeping cybersecurity measures up to date, but the Ohio law will likely be more effective in protecting consumer data by maximizing incentive to adopt cybersecurity measures.

Thus, the Ohio Data Protection Act's implementation of an affirmative defense will be more effective protecting consumer data than other approaches due to its incentivizing approach. Additionally, the Ohio law will be an effective resource in the cybersecurity landscape because it does not act as a complete bar to litigation.

ii. The Act Will Not Bar Consumers from Using Litigation as a Form of Redress

The Ohio Data Protection Act will not serve as a bar to consumers whose information is improperly handled because it only serves as an affirmative defense for tortious claims and will only be implemented when covered entities do not comply with the enumerated standards. One concern expressed by critics of the Ohio Data Protection Act, is that it will not allow consumers to pursue claims against covered entities by barring their claims.[115] Essentially, opponents of the Act argue that it will not permit litigants to get past the motion to dismiss stage of litigation due to the option covered entities have to assert the affirmative defense. The argument follows that consumers will not be able to recover from companies who have allowed data to be improperly accessed. While this argument does point to the Ohio Data Protection Act's largest shortcoming, it fails to take into consideration two key aspects of the Act involving its limitation to tortious suits and the inapplicability of the affirmative defense to covered entities who do not meet the requisite standards.

First, the Ohio Data Protection Act's affirmative defense only applies

114. Ohio Rev. Code Ann. § 1354.03(D), *supra* note 60.

115. Mark Abramowitz, *Testimony in Opposition to Senate Bill 220*, DICELLO LEVITT & CASEY, 4 (June 26, 2018), https://www.dlcfirm.com/mark-abramowitz-testifies-ohio-cybersecurity-safe-harbor-bill/.

to tortious claims relating to the mishandling of consumer information.[116] Many plaintiffs in class action lawsuits bring contract claims based on the theory that the entity who is holding the information has a contractual obligation to protect it and has failed to do so.[117] For instance, in the *Yahoo* case discussed above, the California district court denied Yahoo's motion to dismiss on both negligence claims and claims rooted in contract law.[118] While this case may have come out differently if the Ohio law was applicable in terms of the negligence claim asserted by the class action, the affirmative defense would have been ineffective for the contract claims. Thus, the Act only bars tortious claims, like negligence, and leaves the door open for plaintiffs to assert claims based in contract, or some other applicable law.

Second, the Ohio Data Protection Act only bars tortious claims where the entity asserting the affirmative defense can prove that it satisfied the enumerated requirements involving industry recognized standards or applicable federal law.[119] If the covered entity is not able to fulfill this burden, the affirmative defense is not applicable, and tortious claims asserted against the covered entity will not apply. Additionally, entities that cannot meet this burden may be more likely to be negligent in their handling of sensitive information. Thus, the Act does not bar tortious claims that may have meritorious arguments, but only protects covered entities who follow applicable, updated industry recognized frameworks or federal law.

Therefore, the Ohio Data Protection Act will not serve as a complete bar to those who seek recourse for the harm suffered by the mishandling of personal information through the courts. Rather, the Act offers an approach that leaves alternative options open for plaintiffs and takes into consideration covered entities' efforts to protect private information. The positive effects that this law will likely have for businesses and consumers may be influential as other states consider cybersecurity legislation.

IV. CONCLUSION

Even though the law was enacted with sound policy underpinnings, time will tell whether Ohio's decision to enact a safe harbor as a means of encouraging covered entities to adopt more protective cybersecurity

116. *Final Analysis: Sub. S.B. 220*, at 1, *supra* 35.

117. Wayne M. Alder, *Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend a Claim*, BECKER & POLIAKOFF, 5 (last accessed on Feb. 13, 2019), https://beckerlawyers.com/wp-content/uploads/2018/02/20151001_alder_data_breaches.pdf.

118. In re: Yahoo Data Breach, 313 F.Supp.3d at 1150.

119. *Final Analysis: Sub. S.B. 220*, *supra* note 35.

measures will be effective. One source stated that the Ohio Data Protection Act could very well serve as a bellwether for other states looking to address an increasing number of data breach suits.[120] Other states will likely follow Ohio's lead, however, only if the law protects consumer data and reduces the number of lawsuits filed in the aftermath of a data breach.[121] More significantly, it is important to remember that very little has been done on the federal level to address the cybersecurity issue. This, however, may be changing. On November 16, 2018, President Donald Trump signed a bill bestowing the responsibility of overseeing civilian cybersecurity protection to the Department of Homeland Security.[122]

This action demonstrates the ever-increasing significance of cybersecurity concerns on the national stage as the Cybersecurity and Infrastructure Security Agency will be elevated to the same level as other agencies included within the Department of Homeland Security, including the Secret Service and the Federal Emergency Management Agency.[123] The development of federal legislation or regulations may be exceptionally valuable in terms of setting specific standards or requirements for entities who handle consumer information. Federal action would also address the piecemeal approach adopted by the states by creating a more uniform landscape.

Should the federal government continue to address cybersecurity concerns, however, the abundance of types of legislation and regulation implemented by the states may be helpful in terms of setting a national course. The federal government may very well consider the Ohio Data Protection Act as a useful experiment that implements a unique approach to addressing cybersecurity issues and protecting consumer information. Thus, the effectiveness of the Ohio Data Protection Act may prove influential if and when the federal government decides to promulgate additional cybersecurity law.

120. Sara Merken, *Companies Could Sidestep Data Breach Claims Under Ohio Law*, BLOOMBERG LAW, (Oct. 31, 2018), https://www.bloomberglaw.com/document/XACVHQAS000000?bna_news_filter=us-law-week&jcsearch=BNA%252000000016683cbdbd4a96ea7dfd20f0002#jcite.

121. *Id.*

122. Olivia Beavers, *Trump Signs Bill Cementing Cybersecurity Agency at DHS*, THE HILL, (Nov. 16, 2018), https://thehill.com/policy/cybersecurity/417185-trump-signs-bill-cementing-cybersecurity-agency-at-dhs.

123. *Id.*