PROMOTING BETTER CYBERSECURITY

An Analysis of the Ohio Data Protection Act

MARCH 25, 2019

DENNIS HIRSCH

Professor of Law / Faculty Director, Program on Data and Governance
The Ohio State University Moritz College of Law

BRIAN RAY

Professor of Law / Director, Center for Cybersecurity and Privacy Protection
Cleveland-Marshall College of Law

KEIR LAMONT

Program Manager, Program on Data and Governance
The Ohio State University Moritz College of Law

THE OHIO STATE UNIVERSITY
MORITZ COLLEGE OF LAW

CLEVELAND STATE UNIVERSITY
CM LAW
Cleveland-Marshall College of Law

Table of Contents

I. Executive Summary 1

II. Background 3

III. Analysis of the ODPA 4

A. Scope 7

B. Protected Information 7

C. Demonstrating Reasonable Conformity 8

1. Cybersecurity Frameworks 8

2. Third-Party Attestations and Formal Certification 10

3. Cloud Providers 11

4. Continuing Compliance 11

D. Litigation Issues 12

E. Practical Considerations 13

IV. ODPA's Likely Effect 14

A. Promoting Better Cybersecurity 14

B. Potential Benefits 15

I. Executive Summary

The Ohio Data Protection Act ("ODPA" or the Act), came into force on November 2, 2018.[1] The Act seeks to improve cybersecurity among Ohio businesses. It does so by providing an affirmative defense against tort claims arising from a data breach to businesses that can demonstrate they have implemented a qualifying cybersecurity program that reasonably conforms to one of ten specified cybersecurity frameworks and met certain other safeguards specified in the Act.

This White Paper describes the ODPA in detail and analyzes its potential application and effects. It introduces the Act to businesses considering qualifying for the affirmative defense and identifies key open questions regarding the Act's scope and practical utility. It should serve as a resource for businesses, attorneys, judges, policymakers, and compliance professionals interested in learning more about the Act and considering the opportunities that it presents. With some important caveats, our overall conclusion is that the ODPA is likely to provide a modest but meaningful incentive for many Ohio businesses to improve their cybersecurity posture.[2]

The process of qualifying for the ODPA's protection is not fundamentally different from that required to manage cybersecurity risk from an organizational perspective. It also overlaps significantly with the steps many businesses already take to comply with existing data security and privacy regulations. The substantial economic and reputational benefits that flow from a robust cybersecurity program, combined with the protections that the affirmative defense offers against liability for data breach-related tort claims, should make it worthwhile for many businesses to seek the ODPA's protections.

The ODPA's Core Features:

- The Act provides an affirmative defense for tort claims arising out of a data breach and brought in an Ohio court or under Ohio law. It does not apply to other potential claims, including breach of contract or statutory claims. The Act does not establish any minimum standards for data security or privacy or provide a basis for any private right of action.
- To qualify for the affirmative defense, a business must maintain and comply with a cybersecurity program that meets four, overlapping requirements. The company's cybersecurity program must: (1) contain administrative, technical and physical safeguards for the protection of covered information defined in the Act; (2) reasonably conform to one of ten cybersecurity frameworks; (3) be designed to protect covered information across three, specified dimensions; and (4) be appropriate in scale and scope considering the business's size and complexity, the nature and scope of its activities, the resources available to it, the sensitivity of the information to be protected, and the cost and availability of tools to improve information security and reduce vulnerabilities.
- Demonstrating conformity with one of the listed cybersecurity frameworks is the key requirement for a business to qualify for the Act's protection and will, in most cases, largely satisfy the other requirements.

1 Ohio Attorney General's Office, "Senate Bill 220: The Data Protection Act" (last accessed: Dec. 16, 2018), www.ohioattorneygeneral.gov/Business/CyberOhio/Data-Protection-Act.

2 The analysis in this paper represents the views of the individual authors not those of any organization or institution. This documents is intended as a general discussion of the Ohio Data Protection Act and does not constitute legal advice.

- There are two categories of covered information in the Act: (1) "Personal Information," which includes data that could, on its own, be used to identify a person; and (2) "Restricted Information," which broadens the scope of the Act's protection to include data that could, in combination with other data, be used to identify a person.
- The ODPA specifies six general industry frameworks and four federal laws or regulations to which a business may reasonably conform so as to qualify for the affirmative defense. Only a business regulated by one or of the four listed federal laws may qualify by conforming to that law's requirements.[3] Others must qualify by conforming to one of the six general frameworks. In data breaches involving data covered by the Payment Card Industry Data Security Standard (PCI-DSS), businesses that wish to qualify for the affirmative defense must demonstrate conformity both with PCI-DSS and with one of the six general industry frameworks.

Practical Considerations:

- The ODPA's requirements and the frameworks it specifies enable a business to tailor its cybersecurity program to its size, scope and resources so long as the entity structures the program so that it reasonably protects covered information.
- Most businesses subject to one of the regulatory frameworks specified in the ODPA should be able to meet the Act's requirements without much additional effort but may need to take some additional steps to ensure their program is sufficiently comprehensive.
- Proving the defense in court likely will require an extensive factual record and expert testimony showing that the cybersecurity program has satisfied the ODPA's requirements and reasonably conformed to one of the listed frameworks.
- A business should carefully document the steps it takes to develop, implement and maintain its cybersecurity program, including: (1) its process and criteria for identifying whether it possesses information of the type that the Act addresses; (2) how it designed its program for protecting that information; and (3) its process for ensuring ongoing compliance with its program throughout the business.
- Qualified cybersecurity professionals can attest that a business's program satisfies the cybersecurity framework it selects. In addition, several of the frameworks allow for a formal attestation of compliance. Such an attestation should significantly assist in asserting the defense but may not be sufficient on its own.
- Many cloud service providers maintain certified compliance with a number of the cybersecurity frameworks that the ODPA recognizes. A businesses that utilizes such a cloud services provider can use the provider's certified compliance with a recognized framework to show its own reasonable conformity with that framework. This can be a cost-effective way to develop a qualifying cybersecurity program, at least with respect to data that the company stores with the cloud services provider. A company that uses such an approach will still need to ensure that its own program provides comprehensive protection for covered data in all other relevant areas.

3 O.R.C. § 1354.03

II. Background

Data breaches have become increasingly common, larger, costlier to businesses, and more harmful to consumers.[4] Small and medium-sized businesses can find it challenging to keep up with emerging cybersecurity threats and best practices. In a 2018 survey, 67% of small and medium-sized businesses reported experiencing a cyber-attack in the past year, yet only 28% rated as "highly effective" their ability to mitigate such threats, vulnerabilities and attacks.[5] In response to these trends, many states have passed new cybersecurity and privacy laws that require companies in particular industry sectors to meet or exceed baseline cybersecurity standards and/or take particular actions (e.g. timely notice to data subjects) in the event of a data breach.[6]

The Ohio Data Protection Act is unique among state laws seeking to improve data security. Instead of setting minimum cybersecurity standards or imposing new penalties, the Act provides an incentive for businesses to create, maintain, and comply with a cybersecurity program that conforms to industry best practices. The Ohio Attorney General has said that the Act seeks to encourage businesses voluntarily to "invest in strong cyber security controls" allowing consumers to be "confident that their personal information will be better protected."[7]

The ODPA was the first legislative proposal drafted by Ohio Attorney General Mike DeWine's CyberOhio Program.[8] Attorney General DeWine launched CyberOhio in 2016, describing it as a collection of cybersecurity initiatives aimed at fostering a "legal, technical, and collaborative cybersecurity environment to help Ohio businesses thrive." The CyberOhio program encompassed five initiatives, including the creation of an Advisory Board comprised of industry experts and business leaders to advise the Attorney General's Office on cybersecurity initiatives, and exploring draft legislation "to improve the legal cybersecurity environment in Ohio for businesses and consumers."[9]

Ohio State Senators Bob Hackett (R – London) and Kevin Bacon (R – Minerva Park) proposed the bill that ultimately became the Ohio Data Protection Act (ODPA) as S.B. 220 in December 2017.[10] Over the course of six months, the bill went through five hearings before the Senate Committee on Government Oversight and Reform Committee and three hearings before the House Committee on Government Accountabili-

4 *See* Juliana De Groot, "The History of Data Breaches," Digital Guardian (Nov. 12, 2018), https://digitalguardian.com/blog/history-data-breaches.

5 Ponemon Institute, "2018 State of Cybersecurity in Small & Medium Size Businesses" (Nov. 2018) available at: http://start.keeper.io/2018-ponemon-report.

6 *See* e.g., National Conference on State Legislatures, "Data Security Laws | Private Sector 2018 report" (Oct. 15, 2018), www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.; N.Y. Comp. Codes R. & Regs. tit. 23, § 500.00, "Cybersecurity Requirements for Financial Services Companies;" 201 C.M.R. § 17.00, "Standards for the Protection of Personal Information of Residents of the Commonwealth;" and 2018 Cal. Legis. Serv. Ch. 886 (S.B. 327) (WEST).

7 Ohio Attorney General's Office, "Bill Launched by Attorney General's CyberOhio Initiative Signed into Law," Press Release (Aug. 3, 2018), www.ohioattorneygeneral.gov/Media/News-Releases/August-2018/Bill-Launched-by-Attorney-General%E2%80%99s-CyberOhio-Init.

8 Mike DeWine has served as Ohio Attorney General since January 2011. He became Ohio Governor on January 14, 2019.

9 Ohio Attorney General's Office, "Attorney General DeWine Launches CyberOhio Initiative to Assist Ohio Businesses," Press Release (Sept. 29, 2016), www.ohioattorneygeneral.gov/Media/News-Releases/September-2016/Attorney-General-DeWine-Launches-CyberOhio-Initiat.

10 The Ohio Legislature, "Senate Bill 220, Committee Activity" (Last accessed: Dec. 16, 2018), www.legislature.ohio.gov/legislation/legislation-committee-documents?id=GA132-SB-220.

ty and Oversight.[11] Seventeen different witnesses testified at these hearings, ten who favored passage and seven who opposed the bill. Opponents argued that the listed cybersecurity frameworks were overly flexible, the technical issues involved would require judges to become security experts and increase litigation costs by requiring expert testimony on both sides, and that the affirmative defense would discourage plaintiffs from bringing data breach claims in Ohio.[12]

The Act passed unanimously in the Ohio Senate but faced a closer vote in the Ohio House (68-23), where it was unanimously supported by Republicans but opposed by 80% of the House Democratic Caucus.[13] Governor Kasich signed the Act into law on August 3, and the Act became effective on November 2, 2018.

III. Analysis of the ODPA

When a business experiences a data security breach, those affected by the breach sometimes bring a tort suit against it seeking damages. The ODPA focuses on that situation. It identifies a number of accepted cybersecurity standards. Where, prior to the breach, a business develops and implements a cybersecurity plan that reasonably conforms to one of these standards, the Act provides it with an affirmative defense against the tort suit. In this way, it seeks to encourage more businesses voluntarily to adopt and conform to one of the accepted cybersecurity standards.

To accomplish this, the Act states that any business that "accesses, maintains, communicates, or processes personal information or restricted information,"[14] that reasonably conforms to a recognized cybersecurity standard (and meets certain other criteria, described below), and that suffers a data security breach, may assert an affirmative defense to "any cause of action sounding in tort" that "alleges that the failure to implement reasonable information security controls resulted in a data breach."[15]

The Act defines "data breach" as "unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information or restricted information" of a covered entity that "causes, reasonably is believed to have caused, or reasonably is be-

11 *Id.*

12 *Id.* Several of these witnesses testified at more than one hearing. Proponents included the Ohio Manufacturer's Association, the Ohio Chamber of Commerce, and the National Federation of Independent Business and opponents included the National Association of Consumer Advocates and the Ohio Association for Justice.

13 The Ohio Legislature, "Senate Bill 220, Votes" (last accessed: Dec. 16, 2018), www.legislature.ohio.gov/legislation/legislation-votes?id=GA132-SB-220. Several changes were made to the original draft bill as it moved through the legislative process. First, initially the affirmative defense applied to "personal information" improperly disclosed in a data breach. The enacted version expanded the information a cybersecurity program is required to protect by adding the category of "restricted information," which includes any unencrypted information that could be combined "to distinguish or trace the individual's identity or that is linkable to an individual" and present a risk of identity theft or other fraud. Second, the original bill required that a business prove "substantial compliance" with a specified framework in order to assert the defense. However, due to concerns that several of the frameworks were not drafted for businesses to demonstrate "compliance," the enacted version instead requires an entity to "reasonably conform" to one of the listed frameworks.

14 The Act uses the term "covered entity" to refer to such businesses. A "covered entity" is a "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 outside this state." O.R.C. § 1354.01(B). A "business" is "any limited liability company, limited liability partnership, corporation, sole proprietorship, association, or other group, however organized and whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, or the parent or subsidiary of any of the foregoing." O.R.C. § 1354.01(A).

15 O.R.C. §§ 1354.02(D)(1) and (2).

lieved will cause a material risk of identity theft or other fraud to person or property."[16]

To qualify for the affirmative defense, a business must meet four substantially overlapping requirements:

1. First, it must "create, maintain and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards" for the protection of "personal information"[17] or of both personal information and "restricted information"[18]

2. Second, the cybersecurity program must "reasonably conform[] to an industry recognized cybersecurity framework."[19]

3. Third, the program must be designed to protect: (1) "the security and confidentiality of the relevant information"; (2) "against threats to the security or integrity of the information"; and (3) "against unauthorized acquisition of information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates."

4. Fourth, the "scale and scope" of the program must be based on all of the following: the entity's size and complexity; the nature and scope of its activities; the sensitivity of the relevant information; the cost and availability of tools to protect the information; and the business's available resources.

The second of these—that a business reasonably conform to one of the listed cybersecurity frameworks—is the core requirement. Companies that meet this criterion will likely have gone a long way towards meeting the other three. For example, the HIPAA Security Rule requires a covered entity to "maintain reasonable and appropriate administrative, technical, and physical safeguards" to protect electronic protected health information.[20] A company that meets this standard will stand a good chance of also meeting the first ODPA criterion which requires companies to adopt "administrative, technical and physical safeguards" to protect personal and/or restricted data. Likewise, the HHS general guidance, "Security 101 for Covered Entities" breaks down "HIPAA Security" into three components that require essentially the same three things listed in the ODPA's third requirement: confidentiality, integrity and authorized access to protected information.[21] Thus, conforming to HIPAA thus also likely will meet the first and third requirements.

That said, there may be instances in which reasonable conformity to a recognized framework will not result in a business meeting the other

16 O.R.C. § 1354.01(C).

17 Personal Information is "an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: (i) Social security number; (ii) Driver's license number or state identification card number; (iii) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account." ORC § 1354.01(D) citing O.R.C. § 1349.19.

18 Restricted Information is "any information about an individual, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to an individual, if the information is not encrypted, redacted, or altered by any method or technology in such a manner that the information is unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to person or property." O.R.C. § 1354.01(E).

19 O.R.C. § 1354.02(A).

20 45 C.F.R. § 164.530(c)(1). The Department of Health and Human Services provides a separate guidance paper for each of these three safeguards to assist covered entities in complying with them, https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

21 Department of Health and Human Services, "Security 101 for Covered Entities," at 1, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf?language=es.

three ODPA criteria. For example, if the business that complied with the HIPAA Security Rule possessed personal information that was not protected health information, it might have to adopt supplemental safeguards with respect to this additional information. Thus, in addition to demonstrating reasonable conformity with a listed framework, a business must always consider whether it should take any additional steps to ensure it has all the safeguards in place for all of the personal and/or restricted information in its possession and so meets all four ODPA criteria.

The fourth criterion—that the business calibrate the "scale and scope" of its program based on its size and complexity, the nature and scope of its activities, the sensitivity of the relevant information, the cost and availability of tools to protect the information, and the business's available resources—informs how each of the first three requirements applies to a given business. The "scale and scope" factors that the statute identifies reflect the inherent flexibility of the specified frameworks.[22] In many situations, the frameworks will permit smaller businesses with fewer resources to argue that they qualify for the defense with a less extensive cybersecurity program than they will require for a larger, better-resourced company. In addition to a company's size or level of resources, the sensitivity of information that it possesses, and the nature and scope of its activities, can also affect the required scale and scope of its cybersecurity program. The statute does not specify how to balance these potentially competing factors.

The Act identifies three different ways that a business can reasonably conform to an industry cybersecurity framework. First, a business may demonstrate that its program reasonably conforms to the current version of the following general industry frameworks:

- NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)
- NIST Special Publication 800-171
- NIST Special Publications 800-53 and 800-53a
- The FedRAMP Security Assessment Framework (FedRAMP SAF)
- The Center for Internet Security's "Critical Security Controls for Effective Cyber Defense" (CIS Controls)
- The ISO/IEC 27000 Family - Information Security Management Systems[23] (ISO 27000 Family)

Second, a business that is already subject to the cybersecurity requirements contained in one of the following laws or regulations may demonstrate that its program reasonably conforms to that law's requirements. The four laws or regulations are:

- The Health Insurance Portability and Accountability Act security requirements (HIPAA)
- The Gramm-Leach-Bliley Act Title V (GLBA)
- The Federal Information Security Modernization Act of 2014 (FISMA)
- The Health Information Technology for Economic and Clinical Health Act (HITECH)[24]

Finally, a business that already must comply with the Payment Card Industry Data Security Standard (PCI DSS) m[25]ay qualify for the affirmative defense if it shows that it "reasonably complies" with the PCI DSS and, in addition, reasonably conforms to one of the first six identified cybersecurity frameworks.

22 For example, HITECH and the HIPAA Security Rule lists a similar set of factors.
23 O.R.C. § 1354.03(A)(1)(a)-(f).
24 O.R.C. § 1354.03(B)(1)(a)-(d).
25 O.R.C. § 1354.03(C).

When a cybersecurity framework or federal law that a business is using as the basis for asserting the affirmative defense is revised or amended, the business has one year following the publication or effective date of the new version to update its cybersecurity program.[26]

A. Scope

The ODPA's affirmative defense is available to any business that maintains a qualifying cybersecurity program, regardless of that business' sector, size, service-type, business model, and whether web-based or brick-and-mortar.

The affirmative defense provides protection against tort claims asserted in data-breach related litigation. Consumer data breach class actions typically involve a number of tort claims, including negligence and fraud, but also often include other claims not covered by the defense, such as breach of contract or unjust enrichment.[27] As a result, the defense, which only governs tort claims, may not protect against all claims in a consumer action. Nonetheless, the substantive steps a business takes to qualify for the defense should better position it to defend itself on the merits against these other claims and also to respond to regulatory investigations that frequently accompany data breach class actions.

The defense is limited to tort claims under Ohio law or brought in Ohio courts. This language potentially expands its application in two ways that raise interesting jurisdictional and conflict-of-laws issues that courts will need to address. First, in Ohio courts it appears to displace normal choice-of-law principles by making the defense available to any tort claim. Second, it makes the defense available in actions outside of Ohio where the court determines that Ohio's substantive law applies.

B. Protected Information

The ODPA recognizes two categories of protected information. The first, "Personal Information," is directly imported from Ohio's Security Breach Notification Act which defines it as an individual's name in combination with that person's social security number, driver's license or state ID card number, or credit card number or account number along with the code allowing access to the individual's financial account.[28]

The second, "Restricted Information," broadens the Act's scope to include "any information that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to an individual… and the breach of which is likely to result in a material risk of identity theft or other fraud to person or property."[29] As this definition makes clear, "restricted information" encompasses information that, if the subject of a breach, is "likely to

26 O.R.C. §§ 1354.03(A)(2), (B)(2), & (C)(2).

27 *See*, e.g., Allens-Linklaters, "A global snapshot of data breach class actions," (Oct. 1, 2018), https://www.allens.com.au/pubs/priv/pulse-1810/article-03.htm (summarizing the claims brought in several large consumer data breach class actions).

28 *See* O.R.C. 1349.19, defining Personal Information as consisting of an individual's name linked to a Social Security Number, State ID Number, or financial account + access code.

29 The "Restricted Information" category potentially expands the ODPA's protection to tort claims based on disclosure of a much broader range of potentially sensitive information. A prominent trade association criticized this change arguing that it would "cause companies to divert cybersecurity resources from protecting sensitive personal information." (Jim Halpert, "Oppose SB220, Cybersecurity 'Safe Harbor' Legislation," State Privacy and Security Coalition (June 25, 2018)).

result in a material risk of identity theft or other fraud to person or property."[30] This additional requirement limits to some extent the otherwise expansive scope of the "restricted information" category.

In combination, "personal information" and "restricted information" appear to encompass all categories of information that, if improperly disclosed, could form the basis of a tort claim. Businesses seeking to qualify for the defense will need carefully to assess what information might be covered.

C. Demonstrating Reasonable Conformity

1. Cybersecurity Frameworks

In choosing specific cybersecurity frameworks to include in the Act, the Ohio Legislature, with guidance from CyberOhio, had several priorities. As a generally applicable law, the frameworks would have to apply to, and be implementable by, differently situated businesses with radically different cybersecurity risks and needs. Therefore, the Legislature sought to include frameworks that avoided designating prescriptive, one-size-fits-all, "check the box" requirements. It opted instead for descriptive frameworks that include risk-assessments and cybersecurity protocols scalable to the particularized needs of a business. Testifying in support of the legislation, Ohio Attorney General Mike DeWine explained that the chosen frameworks are intended to:

1. Be customizable for use by any type of business;
2. Contain guidance that can cover all aspects of a business' cybersecurity program;
3. Require businesses to remain vigilant and evaluate and implement new cybersecurity technologies and practices in order to remain reasonably compliant with a recognized framework;
4. Represent the most popular cybersecurity frameworks currently used in industry;
5. And "contain extensive industry-recognized security controls that guard against fluctuating cyber threats."[31]

To encourage businesses to make the desired investments in their cybersecurity programs, the costs of implementing the frameworks was also a factor in their selection.

As described above, the Act lists three ways that a business can reasonably conform to a framework. The first, set out in Section 1354.03(A), permits businesses to conform to one of six general frameworks. These six frameworks are generally applicable, flexible, and scalable.[32] They describe hundreds of potential security controls that diverse businesses may consider and use as the basis of building a cybersecurity program. While certain frameworks were initially designed for protecting particular categories of data in particular industries,[33] their current versions explicitly recognize that a broad array of businesses may benefit from using the frame-

30 Several recent cybersecurity and privacy laws such as the GDPR and CCPA have also recognized this threat but have responded by crafting expansive definitions of "personal data/information." *See* GDPR Art. 4(1) and Cal. Civ. Code § 1798.140(o)(1).

31 Mike DeWine, Testimony in Support of SB 220, (May 16, 2018), *available at:* www.legislature.ohio.gov/legislation/legislation-committee-documents?id=GA132-SB-220.

32 Among the recognized cybersecurity frameworks, FedRAMP SAF is arguably the odd-one-out, which is specifically designed for Cloud Service Providers hosting federal data.

33 For example, NIST CSF was designed for critical infrastructure and NIST SP 800-171 was designed for Controlled Unclassified Information residing in non-Federal systems.

work to guide their cybersecurity programs. Several frameworks also contain sections that chart comparable items to promote interoperability with one another. The standards for each listed framework vary to some degree in complexity and specificity of requirements.

The Act also provides a second way that some companies can reasonably conform to a framework. Section 1354.03(B) identifies four federal laws (the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, and two others) and states that companies already regulated by these laws may obtain the affirmative defense by virtue of their reasonable conformity to that law or regulation.[34] By including this second pathway, the Legislature likely intended to avoid situations in which one of the listed laws would require a company to meet its cybersecurity standard, and the ODPA would then require that company to meet a separate standard in order to benefit from the affirmative defense. This provision makes clear that required compliance with the listed law also will enable the company to qualify for the affirmative defense. The company does not need to meet two separate standards.

The provision states that it applies to businesses "regulated by the state, by the federal government, or both."[35] This broad language could lead some to conclude that any company regulated under *any* federal or state law could use compliance with one of the four listed laws to obtain the affirmative defense.[36] However, the Legislature's intent with respect to this provision counsels limiting this second compliance path to those companies that are *already regulated by the laws named in the provision*. A reading that did not limit this pathway to these companies, but rather allowed any company regulated under state or federal law to utilize it, would allow virtually any company to take advantage of the provision since all companies are regulated by some state or federal law or another. If the Legislature intended this, it could simply have included the four federal laws in its initial list of acceptable cybersecurity frameworks.[37] The fact that it did not do this suggests that the courts should read the phrase "regulated by the state, by the federal government, or both" to mean regulated by one of the four listed laws.[38] Companies not already regulated by these laws will have to utilize the other compliance methods.

Another question is whether an organization subject to one of the listed regulations is restricted to demonstrating conformity with the law or regulation that covers it. As a practical matter that may be the simplest route for such organizations. But the general requirements in section 1354.03, combined with section 1354.03's permission to demonstrate reasonable conformity under any of the three routes, suggest that a regulated organization instead could choose to demonstrate conformity with one of the general frameworks.

Notably, the Act does not specify what it means to conform to these regulatory frameworks. It is likely that courts will look not only to the bare text of the laws and regulations listed but also to the substantive requirements and considerations that have been developed through agency regulation, guidance, reporting, and enforcement actions.[39] Moreover, as noted above, a business

34 O.R.C. §1354.03(B).

35 *Id.*

36 *See* Vincent Pitaro, "Ohio Adopts Pioneering Cybersecurity Safe Harbor for Companies" The Cybersecurity Law Report (Sept. 19, 2018).

37 O.R.C. § 1354.03(A)(1).

38 The enacted version of the ODPA lists only federal laws begging the question why the provision includes businesses regulated by state and federal law. An earlier version of the bill included language permitting businesses to demonstrate conformity with other equivalent industry cybersecurity frameworks, which would have included frameworks established by state law.

39 HIPAA and HITECH specify 18 standards and 36 general implementation specifications and only apply to personal

relying on conformity with one of these laws must ensure that its program also meets the Act's other requirements.

The third option—often dubbed "PCI-DSS-plus"—requires businesses that are covered by the Payment Card Industry Data Security Standard (PCI-DSS) reasonably to conform both to this standard and to one of the six industry cybersecurity frameworks. Some commentators have questioned why this provision was included when it appears to require more extensive efforts than the others.[40] A reasonable reading of this provision is that, whenever a breach involves PCI-related information, a business will be required both to demonstrate reasonable conformity with PCI and with another framework to qualify for the affirmative defense.[41] This makes practical sense because the business necessarily will have been subject to PCI-DSS in any case but PCI-DSS is much more limited in scope than the other regulatory frameworks the Act includes.

2. Third-Party Attestations and Formal Certification

While courts are well practiced in applying reasonableness standards, determining reasonable conformity with a cybersecurity framework will be a relatively novel interpretive exercise for most judges.[42] As such, businesses should to take affirmative, documentable steps to demonstrate reasonable conformity with a recognized framework. Several of the listed frameworks provide for formal certification and most of the others provide substantial guidance for assessing an organization's security posture.

The Act does not require certification or an independent attestation to demonstrate reasonably conformity with the listed frameworks. Nonetheless, obtaining certification or an attestation from a qualified professional provides some clear benefits. Although it likely will not be sufficient by itself, it will lay a foundation for demonstrating reasonably conformity to the specified framework. By the same token, those businesses that fail to seek certification where it is available may raise doubts regarding whether their program would have met the framework's requirements.

Two frameworks, the FedRAMP SAF and the ISO 27000 Family specifically provide for third-party certification of compliance, and the NIST frameworks listed have associated "self-assessment frameworks" for developing and analyzing security control assessments. Conducting these self-assessments, however, generally requires considerable expertise and may require outside assistance.[43]

The Act also does not specify a process for demonstrating that a business has included the general safeguards and protections listed in section 1354.02 or for certifying that the scale and scope is appropriate. The substantial overlap

health information. GLBA Title V and FISMA provide no specific security controls, but instead empower other authorities to establish appropriate cybersecurity standards for regulated entities.

40 *See* Wool, *supra* note 26.

41 As discussed in the next section, this does not necessarily require formal certification under either PCI or the other frameworks.

42 Though, as Attorney General DeWine noted in testimony, 13 other states require that states implement "reasonable cybersecurity standards." *See* DeWine, *supra* note 40.

43 For example, NIST SP 800-171A provides for "assessment procedures to help organizations determine compliance to the security requirements that can be used to generate relevant evidence to determine if the security safeguards employed by organizations are implemented correctly, are operating as intended, and satisfy the CUI security requirements." NIST 800-53 emphasizes that compliance requires "using all appropriate information as part of an organization-wide risk management program" and the effective use of "the tailoring guidance and inherent flexibility in NIST publications so that the selected security controls documented in organizational security plans meet the mission and business requirements of organizations."

between these general requirements and the requirements under most of the listed frameworks strengthens the potential value of engaging an independent expert to conduct an assessment and provide an attestation that the program meets both sets of requirements.

3. Cloud Providers

Businesses may be able to take significant and cost-effective steps towards qualifying for the ODPA's protection by utilizing a cloud services provider that is itself certified under one of the listed frameworks to host or manage their data. Many cloud service providers, including Amazon Web Services, Google Cloud, IBM Cloud, and Microsoft Cloud Services, maintain certified compliance with multiple cybersecurity frameworks recognized by the Act.[44] These businesses undergo annual audits of their data centers and maintain dedicated compliance personal to ensure ongoing certification to numerous cybersecurity frameworks.[45] Several of these same cloud service providers offer to work with clients to configure their services to meet specific compliance obligations, which could include qualifying for the affirmative defense. That process generally involves identifying which responsibilities and controls the cloud service provider is responsible for implementing and maintaining, and which remain with the contracting business.[46] Therefore, relying on a cloud service provider for infrastructure, application, and storage services could both simplify the process and reduce the burden of creating and implementing a qualifying cybersecurity program under the Act.

That said, employing a certified cloud provider to host and manage data will not in itself either certify a business or directly qualify it for the affirmative defense. The business will still need to develop and implement a plan that both identifies how the services of the cloud provider fit within its overall cybersecurity program and what other measures it has taken to address risk in other aspects of its operation, including local data storage and migration as well as physical security controls. An outside security expert, or sometimes the cloud provider itself, can help to identify which of the ODPA's requirements the cloud provider satisfies, and which remain for the company itself to address.

4. Continuing Compliance

Creating a program that meets these requirements is only first step. A business also must "maintain and comply" with the program. At a minimum, this means that the business will need to show that it regularly updated the policy in response to changes in its own circumstances as well as changes to the framework it has selected. More importantly, the business also will need to ensure that the policy is implemented throughout its operations, including third-parties that have access to protected information.

One of the key issues in litigation will almost certainly be whether the alleged breach was a result of a business's failure to maintain and comply with its cybersecurity program. The reason-

44 *See* e.g., AWS Compliance Programs: https://aws.amazon.com/compliance/programs/ (ISO Family; PCI DSS; FedRAMP; HIPPA; NIST 800-53; 800-171); Google Cloud Standards, Regulation & Certifications: https://cloud.google.com/security/compliance/ (ISO Family; PCI DSS; HIPAA; FedRAMP; NIST 800-53; NIST 800-171); Compliance on the IBM Cloud: https://www.ibm.com/cloud/compliance; (ISO Family; PCI DSS; FedRAMP; HIPPA; FISMA); Microsoft Azure Cloud Compliance Offerings: https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings (NIST 800-171; FedRAMP; ISO Family; HIPPA/HITECH; PCI DSS).

45 *See* Microsoft Trust Center, "Compliance for Microsoft Cloud Services" (last accessed: Dec. 17, 2018), www.microsoft.com/en-us/trustcenter/compliance.

46 *See*, Frank Simorjay, "Share Responsibilities for Cloud Computing" Microsoft Corporation (April, 2017), https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91.

able conformity standard provides flexibility and recognizes that perfect security is an impossible standard. Thus, even where an alleged breach resulted from the temporary failure of a specific control or requirement under the selected framework, a business still should be able to argue that it reasonably conformed in the aggregate to the selected framework and/or that the specific failure was not reasonably avoidable. Whether that argument succeeds will turn on the specific facts in each case and how strictly the trier of fact applies the Act's requirements.

This requirement also makes it unlikely that obtaining certification or an independent attestation of compliance with a specific framework will be dispositive of whether a business reasonably conformed its program to that framework. In addition, some frameworks offer different types of certifications. Certifications that are limited to the program design and do not address implementation clearly will be insufficient to meet the "continuing compliance" requirement. Even where the certification covers implementation of the policy, however, it will at most reflect the state of the business at a given point in time. As plaintiffs are likely to argue that the occurrence of a breach means that the business was not reasonably conforming to its chosen cybersecurity framework, businesses should be prepared to present documented evidence of ongoing conformity with a framework and be prepared to testify as to why a breach occurred despite maintaining and complying with a qualifying cybersecurity program.

D. Litigation Issues

The Act's protections are structured as an affirmative defense. Under both the Federal Rules of Civil Procedure and Ohio's Civil Rules, a defendant must assert an affirmative defense in either a pre-answer motion or in a responsive pleading (or an amendment to that pleading).[47] This ensures that a business asserting the defense bears the burden of providing evidence and proving that its qualifying cybersecurity program meets the Act's requirements.

The option to assert the defense in a pre-answer motion creates a possibility that a defendant business could seek dismissal of a data breach claim on the basis of the defense. This concern was raised by during hearings on the legislation, where critics suggested that the Act would foreclose data breach victims from an opportunity to have their cases meaningfully heard.[48] As explained earlier, however, establishing that a business's program meets the Act's requirements will inevitably raise a range of complex factual and legal questions. Resolving these factual issues will require at least some discovery, and so it's unlikely that a court would dismiss a case on this basis.[49]

In data breach litigation, either party could move for summary judgment on the question of whether the defense applies. Certification under a framework that provides for it and/or an independent attestation of compliance with the Act's requirements could play a significant role at this stage if a court deems it sufficient to meet a defendant's initial burden of production. This would require the plaintiff to identify admissible evidence in the record that the trier of fact could rely on to decide that the business failed to meet the Act's requirements in spite of that certification/attestation.

47 *See* Ohio Civ. R. 8(c), 12; Fed. R. Civ. P. 8(c) and 12.

48 *See* Curtis Fifner, Testimony on SB 220, Ohio Association for Justice (June 26, 2018), *available at:* www.legislature.ohio.gov/legislation/legislation-committee-documents?id=GA132-SB-220.

49 Indeed, Attorney General DeWine stated in his testimony supporting the legislation that "[this] is not a motion to dismiss issue, rather, it will be decided by the trier of fact at trial." DeWine, *supra* note 40.

As an initial matter, there is a strong argument that a court should require a defendant to provide more than independent certification or attestation of compliance to meet its initial burden because the Act requires continuing maintenance and compliance with a qualifying cybersecurity program. It also should not be overly difficult where an alleged breach has occurred for a plaintiff to identify evidence that would demonstrate that a genuine issue over facts material to the defense exists. This makes it likely in most cases that the defense will not dispose of the case at the summary judgment stage.

In theory, the affirmative defense establishes an alternative path for a defendant to demonstrate that it is not legally liable for the damages caused by the alleged breach. Under the affirmative defense, a defendant can avoid liability by proving that it met the ODPA's requirements (including, most importantly, that it reasonably conformed to a recognized cybersecurity framework). Even if it fails to convince the jury (or judge) that it met each of the Act's requirements, the defendant can still argue that it nonetheless should not be liable for the alleged breach because it had a sufficiently reasonable data security program in place. In practice, however, it may be difficult for a jury effectively to distinguish between these two arguments given that the factual issues under both the ODPA and most tort theories are substantially the same.

The technical nature of the factual issues that asserting the affirmative defense raises will almost certainly require expert testimony on both sides. One of the concerns raised during hearings on the Act and in subsequent commentary is that this will result in increased litigation costs.[50] However, data breach litigation typically already involves expert testimony regarding many of the same factual questions, including forensic analysis of the incident itself and the extent to which the business had taken reasonable steps to prevent, resolve, and mitigate it. There will be some more specific issues involved in demonstrating reasonable conformity with a particular framework, but it remains to be seen whether those issues will increase significantly the cost of bringing or defending the suit.

A more realistic concern is that the availability of the defense under Ohio law and in Ohio courts may create an incentive for both sides to forum shop and lead to increased litigation over choice-of-law and other procedural questions. The defense does not by itself establish a basis for establishing personal jurisdiction in Ohio. Thus, while the defense may create a new incentive to litigate jurisdictional questions where they already are present, it does not create new opportunities to contest those issues.

E. Practical Considerations

The steps that a business will take to prepare to assert the affirmative defense in the event of breach-related litigation are not fundamentally different from those that it would follow to manage cybersecurity risk from an organizational perspective. Business considerations should therefore be the primary driver for selecting a designated cybersecurity framework as well as for taking any additional steps to document or certify the cybersecurity program to develop an evidentiary record for the affirmative defense.

Any business seeking to establish eligibility for the defense will need to undertake some version of a cybersecurity risk analysis. Doing so will address the Act's three other requirements and in most cases can also incorporate any more specific requirements that the listed cybersecurity framework designates. A cybersecurity risk

50 See e.g., Abramowitz supra note 13; Fifner supra note 53.

assessment evaluates the security needs of a business and then identifies a range of security controls that the business could implement to manage its risk in a manner acceptable to the business. Frameworks like the ISO 27000 Family further define processes for implementing and testing the effectiveness of the selected controls as well for ensuring ongoing compliance.

It is important to emphasize that, under most of the recognized frameworks, the business will apply a list of factors similar to the general ones included in the Act to determine the acceptable levels of risk. These decisions will then determine the nature and extent of the controls that a business will implement. This process requires substantial expertise to identify the range of relevant risks and to select appropriate controls and implementation processes. While the frameworks provide a set of tools and a process for making these determinations, identifying the relevant level of risk as well as the measures that will manage it to an acceptable level inevitably involves a fair amount of subjective judgment.

Large enterprises seeking to develop a qualifying cybersecurity program may have the resources and internal expertise necessary to undertake a risk assessment analysis and implement a qualifying cybersecurity program themselves. Still, even those businesses might benefit from engaging an outside expert to conduct an independent assessment and provide a written attestation of conformity with the selected framework and compliance with the Act's general requirements. For small and medium sized businesses, it may be necessary to engage third parties to assist in developing a cybersecurity program that qualifies for the affirmative defense.[51]

As was also mentioned above, companies can make substantial progress towards qualifying for the affirmative defense by using a cloud provider that is itself certified under one of the listed frameworks. This can both simplify the process and reduce the burden of creating and implementing a qualifying cybersecurity program under the Act. However, a company will not qualify for the affirmative defense simply by having a certified cloud provider host and manage its data. Such a company still must ensure that its own operations meet the Act's terms. An outside expert and, in some cases, the cloud provider itself, may be able to advise the company on how best to approach this.

IV. ODPA's Likely Effect

A. Promoting Better Cybersecurity

The success of the Act in encouraging businesses to invest in their cybersecurity programs and proactively protect personal and restricted information will be difficult to measure. Absent explicit statements from business leaders, it may be impossible to determine whether the Act is directly causing businesses to expand their cybersecurity programs or is preventing data breaches. However, the Act may emerge as one of many accelerants in the trend of expanding data security programs and cloud migration. Furthermore, while it may be impossible to trace the prevention of a data breach directly back to the Act, companies that maintain a cybersecurity program based on industry best practices will better able to detect, provide respond, recover, and mitigate the harmful effects of a breach that does occur, all of which benefits consumers.[52]

51 Ohio Attorney General's Office, *supra* note 6.

52 *See* Kirk Herath, Testimony in Support of SB 220, Nationwide (Jan. 10, 2018), *available at:* www.legislature.ohio.gov/legislation/legislation-committee-documents?id=GA132-SB-220.

The statute's designation of specific frameworks gives guidance to courts and businesses and may encourage more companies to expand their cybersecurity programs. However, this approach includes two inherent drawbacks. First, it is not possible to predict how industry-standard cybersecurity best practices will change in the future. Therefore, one or more of the designated frameworks may end up lagging behind the others or a new cybersecurity framework may emerge that replaces the Act's recognized frameworks as industry standards. That said, the frameworks that the Act recognizes are frequently updated and are currently widely recognized and used as industry standard best practices.

Second, encouraging businesses to center their cybersecurity programs on complying with a framework (no matter how scalable, responsive, or dynamic) presents an inherent risk of reducing cybersecurity to a formulaic, "check-the-box" endeavor. This business posture can be less effective than maintaining a cybersecurity program that focuses on holistic risk management and innovation. However, as the primary intent of the Act is to increase investment among businesses with limited or no cybersecurity programs, it is highly unlikely that any steps these organizations take to qualify for the affirmative defense will reduce their overall cybersecurity outlook and sophistication.

B. Potential Benefits

In determining whether to create and implement a qualifying cybersecurity program, companies will certainly consider the value that the affirmative defense will provide in the event of a breach. As discussed, the affirmative defense is limited to tort claims involving an alleged data breach in an Ohio court or under Ohio law. The existing data breach landscape presents some significant challenges to consumer class action claims, which potentially limit the value of the ODPA's affirmative defense.[53]

That said, in a 2018 survey corporate counsel predicted data privacy and security class actions will continue to increase and successful consumer actions often result in significant settlements.[54] In addition, businesses will have to consider current and future trends in data breach litigation, including the possibility that courts will recognize new tort theories of liability.[55]

More broadly, good cybersecurity is increasingly good business. Businesses may decide to develop a qualifying cybersecurity program for reasons that extend beyond the Act's affirmative defense. Those that already are regulated under one of the listed frameworks should find it relatively easy to qualify for the Act's protection.

53 *See* Daniel J. Solove & Danielle Keats Citron, "Risk and Anxiety: A Theory of Data Breach Harms" 96 Texas Law Review 737 (2018).

54 *See* Carlton Fields, "The 2018 Carlton Fields Class Action Survey," at 9, https://classactionsurvey.com/pdf/2018-class-action-survey.pdf.; Bronstad, "Yahoo Agrees to Pay $85M to Settle Consumer Data Breach Class Actions," The Recorder (Oct. 23, 2018), www.law.com/therecorder/2018/10/23/yahoo-agrees-to-pay-85m-to-settle-consumer-dat-breach-class-actions.

55 Businesses considering the value of the affirmative defense under Ohio Law will find no readily available statistics on breach litigation in Ohio State courts. The most advanced data breach litigation before federal courts applying Ohio law occurred in Galaria v. Nationwide Insurance. In this case a plaintiff class of 1.1 million consumers whose personal information stolen by hackers in a 2012 breach asserted Fair Credit Reporting Act and negligence claims against Nationwide Insurance. The Court concluded that the causation element of the negligence claim failed pleading standards, stating that the plaintiffs, some of whom did later experience identity theft "at best… have alleged nothing more than time and sequence." However, the Sixth Circuit overruled, finding that the plaintiffs alleged an injury-in-fact, fairly traceable to the conduct of the defendant, "Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints." Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, (6th Cir. 2016).

Even businesses not subject to one of the listed frameworks may choose to market their "Data Protection Act compliant cybersecurity program" as a competitive signal to current and potential consumers, business partners, and cybersecurity insurance companies. The Act's affirmative defense could provide another "arrow in the quiver" for information technology and security professionals arguing for expansion of their company's' cybersecurity programs. Indeed, proponents of the Act noted that it could to reframe discussions of cybersecurity so that companies come to see it as a business investment rather than simply as a cost.[56]

Additionally, businesses will consider the totality of their prospective costs that could result from a security incident. Data breaches are increasingly costly to impacted companies, the global average cost of a data breach has been estimated at $3.68 million, including breach notification costs, lost customer trust, and the expenses of responding to the breach.[57] The Act is likely to prompt businesses to consider seriously their vulnerabilities and all potential repercussions of experiencing a data breach. This may lead to new investments in cybersecurity programs.

As discussed, the ODPA is limited to claims under Ohio law or brought in Ohio courts, which restricts its direct benefit as a defense to liability. There are, however, some encouraging signs that other states may consider similar legislation. The ODPA has garnered significant national attention in the brief time since it has been in effect, and already there are indications that it could serve as a national model. The most promising of these include a working paper drafted by the Conference of Western Attorneys General that endorses Ohio's pro-active approach to promoting better cybersecurity. The paper notes that "some protection from private class action lawsuits is appropriate when a company has taken steps to maintain its cybersecurity" and calls the Ohio approach "laudable."[58] Information Technology professionals, attorneys, and policymakers should remain appraised of efforts to enact similar laws in other jurisdictions.

56 *See* DeWine, *supra* note 40.

57 Ponemon Institute, "2018 Cost of a Data Breach Study: Global Overview" (July, 2018), cf. Sasha Romansky "Examining the costs and causes of cyber incidents," Journal of Cybersecurity (Aug. 25, 2016), *available at:* https://iapp.org/media/pdf/resource_center/Romanosky-cost-cyber-incident.pdf (estimating the cost of a typical cyber incident at less than $200,000).

58 Karen White, "Safe Harbor Working Paper," Conference of Western Attorneys General (Sept. 2018), http://cwagweb.org/wp-content/uploads/2018/09/CWAG-Safe-Harbor-Working-Paper_Final.pdf.