Articles + Publications | December 7, 2023

More Safe Harbor Protections for Navigating Cyber and Privacy Litigation

Privacy & Cybersecurity Newsletter

WRITTEN BY

Hannah Oswald | Molly McGinnis Stine

Cybersecurity and data privacy risks continue to loom large with potentially significant consequences. Litigation, often filed soon after incidents, adds to the possible repercussions. In our previous article, we discussed a trio of states providing affirmative defenses or "safe harbors" that companies can take advantage of to minimize litigation exposure resulting from a data breach. Three other states have recently followed, with Oklahoma, Iowa, and Tennessee recently passing their own "safe harbor" laws.

The first states – Ohio, Connecticut, and Utah – provide that so long as a company develops and maintains a cybersecurity program that meets industry approved frameworks, then that company can assert an "affirmative defense" that will protect it from tort liability if a data breach does occur.

Oklahoma, Iowa, and Tennessee have all recently passed their own legislation that mirrors these "safe harbors." While the Oklahoma, Iowa, and Tennessee statutes were clearly inspired by the prior statutes, each of the new laws has unique variations that may impact how companies and industries approach cybersecurity and data privacy in these states.

Oklahoma: Industry Specific Legislation

On April 26, 2023, Oklahoma passed "The Oklahoma Hospital Cybersecurity Protection Act of 2023" that will become effective in November.[1] The structure and format of the Oklahoma statute largely tracks the Ohio, Connecticut and Utah statutes. For example, like the prior statutes, the Oklahoma statute provides an affirmative defense for covered entities that create and maintain a cybersecurity program that complies with an industry accepted framework. This affirmative defense applies to any claim sounding in tort "alleging that the failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information."[2] Additionally, the scale and scope of a covered entity's program depend on the same factors listed in the Ohio, Connecticut, and Utah statutes.[3] However, while the other state statutes apply generally to all businesses, the Oklahoma statute only provides an affirmative defense to hospitals.[4]

It is not hard to guess what motivated the passage of this statute given that a number of Oklahoma hospitals and their vendors suffered significant cybersecurity incidents in recent years. For example, in the past 18 months alone it's been reported that Duncan Regional Hospital,[5] Avem Health Partners,[6] Oklahoma Institute of Allergy, Asthma & Immunology,[7] and McAlester Regional Health Center[8] all suffered serious cybersecurity attacks that impacted hundreds of thousands of

Oklahoma residents. Given the enormous amount of sensitive data held by these entities, hospitals have been and will continue to be a popular target for hackers. As such, Oklahoma's new statute serves important public policies of (1) incentivizing hospitals to do even more to prevent cybersecurity attacks while also (2) providing a defense for hospitals that limits what could otherwise be massive litigation exposure.

It will be interesting to see whether other states enact similar industry-specific legislation. Industry leaders and trade associations may choose to consider whether their constituents might benefit from targeted legislation. For example, in instances where there is political resistance to or lack of consensus in passing broad legislation, it may be easier to enact an affirmative defense that is limited to a particular high-risk industry. Additionally, targeted legislation could be useful in addressing industry-specific cybersecurity threats or proposing standards that are more tailored to industry concerns.

Iowa: Maximum Probable Loss

Iowa enacted its new affirmative defense on May 3, 2023. The Iowa statute applies to all businesses and provides an affirmative defense to all claims sounding in tort alleging "that the failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information."[9] This affirmative defense also requires businesses to create and maintain a cybersecurity program that conforms to an industry recognized cybersecurity framework.[10] However, Iowa's statute differs from those from Ohio, Connecticut, Utah, and Oklahoma regarding its requirements for the appropriate size and scale of a cybersecurity program.

The other states' cybersecurity affirmative defenses dictate that the size and scope of a program depend on all of the following factors: (1) the size and complexity of the business, (2) the nature and scope of the activities of the business, (3) the sensitivity of the information protected, (4) the cost and available tools to improve information security, and (5) the resources available to the business.[11]

In contrast, the Iowa statute is grounded in the concept of "maximum probable loss." To invoke this affirmative defense, a company must do a calculation every year to determine the "greatest damage expectation that could reasonably occur from a data breach." The cost to operate the business's cybersecurity program must be "no less" than the company's calculated probable maximum loss.[12] In other words, a company must spend at least as much on its cybersecurity program as it expects it could reasonably suffer in damages from a data breach. So if a company believes it could reasonably suffer $1 million in damages from a cybersecurity breach, it must spend at least $1 million on its cybersecurity program to try to prevent breaches.

From a literal perspective, the Iowa statute is certainly different from its predecessor statutes in that it requires companies to do an actual calculation every year regarding likely potential losses. The process of performing these calculations may be beneficial as it makes the issue more tangible for companies. For example, if a company decision maker is not particularly technologically inclined, it may be difficult to explain why a costly cybersecurity program is a necessary and justified expense. Indeed, many CISOs and IT departments have struggled to make meaningful change at companies due to this disconnect.[13] Performing these calculations may help bridge the gap between these departments.

Another characteristic of a maximum probable loss calculation is that it gives the *appearance* of objectivity, while

still providing the company with broad discretion on how to perform the calculations. For example, the statute instructs companies to estimate the "total value of possible damage multiplied by the *probability* that damage would occur."[14] But there is no instruction on how to determine probability, and it is ultimately left to the subjective decision of the company. Companies that are motivated to address cybersecurity threats will likely find a high probability of potential damage. In contrast, companies that are less motivated may find ways to minimize their probability analysis to justify a lower cost for their cybersecurity program.

Overall, while the maximum probable loss calculation appears to be a new requirement, in a more practical sense, it is not notably different than the other statutes' standards for size and scope. The other statutes similarly require companies to weigh a variety of factors related to the cost of the program and the sensitivity of the data. The other statutes also do not instruct companies on how to weigh these competing factors, and both standards provide significant room for discretion as a result.

When these affirmative defenses are eventually litigated, there is likely going to be significant debate about whether a company was reasonable in either weighing the various factors or in calculating their probable loss. As such, it will not be easy for a company to invoke this affirmative defense if it does not create a cybersecurity program. Because "reasonableness" is currently undefined in this context, companies may be well served to keep track of how peer companies are handling cybersecurity and attempt to create their own program that matches a peer of a similar size and scope.

Tennessee: New Privacy Requirements

Tennessee's recently enacted statute includes a "safe harbor" provision but, unlike the other states discussed here, in the privacy – and not the cybersecurity – context. On May 11, 2023, Tennessee passed the "Tennessee Information Protection Act" with new privacy requirements for companies or entities not exempted under the law and meeting certain revenue and other thresholds.[15] For example, the statute has new rules about what personal data companies are allowed to collect, how companies are allowed to maintain that data, and how companies must comply with consumer requests to have data deleted.

The statute also contains a voluntary affirmative defense that is structured in the same manner as the other states' statutes. For example, the affirmative defense will apply to companies that adopt and maintain a privacy policy that complies with the National Institute of Standards and Technology (NIST) privacy framework "or other documented policies, standards, and procedures designed to safeguard consumer privacy." The size and scope of that framework is decided by the same general types of factors listed in the Ohio, Connecticut, Utah, and Oklahoma cybersecurity statutes.[16]

However, in addition to adopting a framework that reasonably conforms to the NIST privacy framework or an acceptable equivalent, a company must also provide consumers with the same substantive rights that are otherwise required under the act.[17] The affirmative defense for this statute is also more narrow in scope as it only applies to claims that are brought under the Tennessee Information Protection Act.[18] Only the attorney general has authority to enforce the act, so the affirmative defense is not applicable to general tort claims brought by consumers.

Next Steps for Cybersecurity and Data Privacy

As technology advances and the legal landscape continues to unfold, there is no doubt that cybersecurity and privacy will continue to be significant issues for companies. At a minimum, companies should evaluate what policies they have in place to prevent and respond to cyberattacks and address privacy concerns. Companies and industries should also track new legislations and rules to stay informed and perhaps comment on or even help create proposed new laws and regulations.

—

[1] Okla. Stat. Ann. tit. 18, § 2068 (West), https://www.oklegislature.gov/BillInfo.aspx?Bill=hb2790&Session=2300

[2] *Id*. at § 2070

[3] *Compare* Okla. Stat. Ann. tit. 18, § 2070 *with* Ohio Rev. Code Ann. § 1354.02(C) *and* Conn. Gen. Stat. Ann. § 42-901(d)(2) *and* Utah Code Ann. § 78B-4-702(4)(c)

[4] Okla. Stat. Ann. tit. 18, § 2069

[5] Sarah Coble, *Oklahoma Hospital Data Breach Impacts 92,000 People*, Mar. 8, 2022, https://www.infosecurity-magazine.com/news/oklahoma-hospital-data-breach/

[6] Jill McKeon, *Third-Party Data Breach Impacts 271K at Oklahoma Healthcare Administrative, Tech Services Company*, Dec. 22, 2022, https://healthitsecurity.com/news/third-party-data-breach-impacts-271k-at-oklahoma-healthcare-administrative-tech-services-company

[7] Katelyn Ogle, Clinic goes offline after alleged cyber security attack, May 17, 2023, https://kfor.com/news/local/clinic-goes-offline-after-alleged-cyber-security-attack/

[8] Stefanie Schappert, *Hackers threaten to auction off DNA patient records from Oklahoma hospital*, July 31, 2023, https://cybernews.com/news/hackers-threaten-to-auction-off-dna-patient-records-from-ok-hospital/

[9] Iowa Code Ann. §§ 554G.1, 554G.2

[10] Iowa Code Ann. §§ 554G.2, 554G.3

[11] *See, e.g.*, Ohio Rev. Code Ann. § 1354.02(C)

[12] Iowa Code Ann. §§ 554G.1, 554G.2

[13] J.C. Gaillard, *Why Companies Should Consider Developing A Chief Security Officer Position*, Jun. 1, 2023, Forbes, https://www.forbes.com/sites/forbesbusinesscouncil/2023/06/01/why-companies-should-consider-developing-a-chief-security-officer-position/?sh=19130def2308; Ellen Flannery, *54% of CISOs are 'fighting an uphill battle' for board-level cybersecurity support*, Jun. 9, 2023, Intelligent CISO, https://www.intelligentciso.com/2022/06/09/54-of-cisos-are-fighting-an-uphill-battle-for-board-level-cybersecurity-suppor/

[14] Iowa Code Ann. §§ 554G.1

[15] Public Chapter No. 408 §§ 47-18-3201 (Tennessee 2023)

[16] *Id.* §§ 47-18-3212.

[17] *Id.* §§ 47-18-3212(a)(2).

[18] *Id.* §§ 47-18-3212(a).

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Privacy + Cyber