Articles + Publications | August 5, 2024

Cybersecurity Safe Harbors – One Step Forward and Two Steps Back

Privacy & Cybersecurity Newsletter

WRITTEN BY

Michael J. McMorrow | Hannah Oswald

Cyberattacks continue to increase in number and severity.[1] This increase has amplified the need for legislation to protect both businesses and consumers. In previous articles,[2] we discussed the few states that enacted "safe harbor" laws companies can leverage to reduce litigation exposure. The trend continues, but with some recent and notable pushback. Recent legislation in states like Tennessee, Florida, and West Virginia introduced new "safe harbors" for private entities, with Tennessee expanding on its previous "safe harbor" legislation. The governors of Florida and West Virginia, however, vetoed the proposed legislation.

Tennessee: New Requirements for Cybersecurity Class Actions

On May 21, 2024, Tennessee amended its cybersecurity "safe harbor" protection by limiting class-action liability for private entities. This "safe harbor" expansion is available to any private entity, including for-profit and non-profit organizations. The amendment imposes strict requirements on plaintiffs seeking to file class-action lawsuits against private entities for cyber incidents.[3] This amendment also raises the threshold for plaintiffs who must now demonstrate that the covered entity acted with intentional disregard or severe lack of care rather than just ordinary negligence. The amendment essentially functions as a precondition that must be met before any liability can be established.

Plaintiffs now face significant challenges when attempting to pursue class action lawsuits after a data breach in Tennessee. The amendment restricts class actions to cybersecurity incidents resulting from "willful and wanton misconduct" or "gross negligence." Negligence alone will not suffice. This heightened threshold requires plaintiffs to prove that the private entity acted with a degree of intent or recklessness that goes beyond negligence, which is a tougher standard to meet. Further, plaintiffs are also required to demonstrate a causal link between the alleged willful misconduct or grossly negligent conduct and the damages incurred.

The amended "safe harbor" protection may benefit entities within the amendment's scope in the event of a data breach or other cybersecurity event that was not caused by the entity's "willful and wanton misconduct or gross negligence." At this time, it is unclear what Tennessee courts consider "willful, wanton, or gross negligence" in the context of cybersecurity. Early cases addressing this development may be instructive to private entities as they seek to take advantage of this "safe harbor" legislation. At minimum, it is critical for private entities to implement robust cybersecurity measures and to create detailed documentation of policies and practices taken before and after the incident.

Tennessee's amended "safe harbor" provision offers a robust shield against unfounded or unsupported claims

and can allow companies to focus on enhancing cybersecurity measures rather than costly litigation. This new amendment highlights the importance of maintaining rigorous cybersecurity practices that are effective and comply with industry and legal standards. As the legal landscape of Tennessee's privacy and cybersecurity laws continues to unfold, a proactive approach to compliance and self-assessment can strengthen a company's defense against potential cyber threats or future litigation.

Florida and West Virginia: Vetoed Safe Harbors

On June 17, the Florida legislature presented the Cybersecurity Incident Liability Act to Gov. Ron DeSantis.[4] The Act sought to provide immunity to counties, municipalities, political subdivisions of the state, and commercial entities from tort claims such as negligence related to a cybersecurity breach so long as they "substantially comply" with certain requirements. This Act would not have provided immunity against claims that might arise out of a breach of contractual obligations related to cybersecurity.

To receive immunity, political entities would have had to comply with the standards set forth in Fla. Stat. 282.3185. If enacted, private entities would have received immunity only if they demonstrated that they: (a) complied with all the notice requirements outlined in the Florida Information Protection Act;[5] (b) "adopted a cybersecurity program that substantially aligns with the current version of any" of several specified third-party frameworks;[6] and (c) continued to "substantially align its cybersecurity program with any revisions" to those frameworks. The Act would not have required "full" compliance with these frameworks, but required private entities to *substantially* align with them, allowing some flexibility in implementations.

That proposed flexibility in the standards proved the bill's undoing. On June 26, Gov. DeSantis vetoed the Act, stating that the "bill could result in Floridians' data being less secure as the bill provides across-the-board protections for only substantially complying with standards."[7] The veto sought to avoid the result of "a consumer having inadequate recourse if a breach occurs." While the Governor's veto suggested that "interested parties coordinate with the Florida Cybersecurity Advisory Council to review potential alternatives to the bill," there is no indication that the Advisory Council has taken any further action in response.

The veto leaves businesses in a precarious position, wherein compliance with third party frameworks that set out industry standards may not necessarily demonstrate meeting any standard of care in a negligence action. The fact of the veto could embolden plaintiffs to test whether frameworks like NIST create a standard and to call into question whether even full compliance with the chosen framework meets the standard of care.

Until the Advisory Council or the legislature provides more drafts or guidance, business entities in Florida may be best served by continuing to aim for thoroughness in their cybersecurity programs, maintaining detailed documentation of cybersecurity practices, and regularly consulting with legal and cyber security experts to ensure ongoing compliance and readiness for potential litigation.

Earlier in May, the West Virginia legislature presented what could have been the West Virginia Consumer Data Protection Act.[8] This presented Act included a "safe harbor" for entities with a comprehensive cybersecurity program. However, Governor Jim Justice quickly vetoed this amendment after it arrived on his desk.[9]

The Act created an affirmative defense for covered entities that created, maintained, and complied with a

comprehensive cybersecurity program. It required covered entities to (1) continuously evaluate and mitigate foreseeable internal and external cybersecurity threats (2) periodically assess the maximum probable loss as a result of a data breach, and (3) ensure cybersecurity measures are proportional to the evaluated risks, entity's size and sensitivity of the data protected. Similarly to Florida's vetoed Act, entities could meet these requirements if they reasonably conformed to one of the listed industry-standard frameworks. The listed frameworks included NIST and CIS. This Act was promising. However, Gov. Justice vetoed this Act because of his concerns regarding "unintended consequences,"[10] and an aversion to immunizing "international entities such as TikTok," as stated in his veto statement.

Despite the West Virginia and Florida vetoes slowing the modest legislative trend seeking to develop "safe harbors" for compliant entities, states legislatures across the country continue to consider ways to encourage public and private entities to strengthen their cybersecurity practices in order to protect consumer data. We will continue to watch for further developments concerning" safe harbor" protections in West Virginia, Florida, and other states.

The Future of Safe Harbor Legislation

As cyber threats evolve, we can expect legislative efforts to follow. Companies should seek to stay informed about future changes in cybersecurity laws and continue to enhance their security protocols to meet the evolving standards. Proactively engaging in these matters will not only help companies take advantage of "safe harbor" provisions but also strengthen their cybersecurity posture.

***

* The authors thank Iris Gomez, a 2025 J.D. candidate at Loyola University Chicago School of Law, for her valuable ?contributions to this article.?

—

[1] Mariah St. John, *Cybersecurity Stats: Facts And Figures You Should Know,* Forbes (Feb. 28, 2024)

https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/

[2] https://www.lockelord.com/newsandevents/publications/2021/10/safe-harbor-ports; https://www.lockelord.com/newsandevents/publications/2023/12/more-safe-harbor-protections

[3] https://legiscan.com/TN/text/HB2434/2023

[4] § 768.401, Fla. Stat. https://www.flsenate.gov/Session/Bill/2024/473/BillText/er/PDF

[5] § 501.171(3)-(6), Fla. Stat.

[6] The frameworks include the National Institute of Standards and Technology (NIST) Framework ?for Improving Critical Infrastructure Cybersecurity, HITRUST Common Security Framework ??(CSF), Center for Internet Security (CIS) Critical Security Controls, and any other similar ?industry framework or standard?.?

[7] R. DeSantis, letter to Sec. of State Byrd, June 26, 2024.

[8] W. Va. H.B. 5338, 2024 Reg. Sess. (vetoed). https://www.wvlegislature.gov/Bill_Text_HTML/2024_SESSIONS/RS/bills/hb5338%20intr.pdf

[9] https://westvirginiawatch.com/2024/03/28/justice-vetoed-eight-bills-passed-by-legislators-this-session-heres-what-they-would-have-done/

[10] *Id.*

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber