POLSINELLI

Publications

February 26, 2025 • Updates

Current Trends in Data Breach Notification Laws: Safe Harbors and Reinforcing the Case for Cybersecurity

The early 2000s marked the start of a new era for consumer protection with the passage of the data breach notification law in California, the first of its kind. Since that time, a patchwork of privacy laws has been enacted across the United States, signaling an ever-greater regulatory shift toward consumer privacy protection. And since the passage of the comprehensive California Consumer Privacy Act of 2018 (CCPA), the United States has seen exponential growth in the number of privacy-related bills being introduced in state legislatures (59 in each of the past two years) as well as the number of bills being passed into law (7 in 2023).[1] This surge in legislative activity has led to a significant increase in both consumer data privacy protections and data breach litigation. This article will first provide a brief update on the state data breach notification laws. Next, it will explore how legislatures and courts are navigating the uptick in data privacy litigation and what the implications are for businesses facing both increased regulation and rising litigation risks.

Updates to State Data Breach Notification Laws

State legislatures continue to update existing data breach notification laws to infuse greater consumer privacy protections. For example, recent updates in Pennsylvania, Florida and Utah add new requirements for companies reporting data breaches, requiring companies to provide complimentary credit monitoring services when certain information is affected (Pennsylvania), increasing regulatory reporting requirements (Pennsylvania and Utah), and expanding the scope of reportable information to include new categories of personal data, including biometric and geolocation data (Florida).

Increased Consumer Litigation

The volume of data breach class action litigation is also growing at a remarkable rate. According to a July 2024 report by Lex Machina,[2] the number of data breach class action cases filed in 2023 nearly tripled the number of such class actions filed in 2022. In fact, in 2023, an average of 170 data breach class actions were filed each month. The total number of data breach class actions filed in the past three years has grown exponentially from just 476 in 2021 to 2,040 in 2023, according to Lex. This increase is believed to be due in part to recent court decisions making it easier for plaintiffs to show standing and successfully prove causation. Just given the volume of such cases handled by our firm in

Related People

- Adam Griffin
- Todd Panciera, Jr.

Related Capabilities

- Data Breach & Incident Response

2024, we expect this growth to continue.

Safe Harbor Provisions

In light of the uptick in data privacy laws favoring consumers and perhaps in response to the exponential increase in data breach class actions, a growing number of state legislatures and courts appear to be attempting to rebalance the scales by creating more favorable outcomes for businesses working to bolster cybersecurity in favor of consumers. This apparent shift away from unnecessarily penalizing businesses who are themselves victims, particularly in cases where actual consumer harm has not occurred, should promote a fairer legal environment. Ohio has led the way as the first state to pass a Safe Harbor provision in 2018 with the passage of its Data Protection Act (DPA). Ohio's DPA provides an affirmative defense in tort-based data breach claims for businesses that implement cybersecurity programs meeting industry-recognized cybersecurity frameworks. According to the legislative notes, the Ohio legislature's aim in writing the law was in part to reduce the likelihood of potential class actions and streamline the court's docket with respect to these matters (i.e., a "legal safe harbor" for compliant businesses)[3] while simultaneously elevating the cybersecurity standards of Ohio businesses.[4]

Tennessee passed a similar law that will go into effect on July 1, 2025. Under Tennessee's Safe Harbor, a private entity is not liable in a class action lawsuit resulting from a cybersecurity event unless the cybersecurity event was caused by willful and wanton misconduct or gross negligence on the part of the private entity.[5]

In Florida, a similar bill passed both the House and the Senate but was ultimately vetoed by Gov. DeSantis.[6] The bill would have shielded an entity from liability in connection with cybersecurity incidents if the entity substantially complied with Florida's data breach notification requirement and adopted a cybersecurity program that substantially complied with several third-party frameworks specified in the bill.[7] In vetoing the bill, DeSantis expressed concern over whether the bill's "minimum cybersecurity standards" could "result in Floridians' data being less secure" and "incentiviz[e] doing the minimum when protecting consumer data."[8] DeSantis invited "interested parties to coordinate with the Florida Cybersecurity Advisory Council to review potential alternatives to the bill that provide a level of liability protection while also ensuring critical data and operations against cyberattacks are protected as much as possible."

Similarly, in West Virginia, Gov. Justice vetoed[9] a bill that, if passed, would have provided entities with an affirmative defense in tort actions alleging that personal information was breached because of an entity's failure to implement reasonable information security controls. For entities to be protected under the bill, they would need to adopt cybersecurity programs meeting the bill's specific requirements or certain industry-specific frameworks outlined in the bill. In vetoing the bill, Justice highlighted the "potential for bad actors to abuse this law and to harm [West Virginia] citizens" and invited stakeholders to help craft a bill that will help the state's businesses while protecting its citizens.

What is clear from these new safe harbor provisions, including those that have failed to pass, is that state governments continue to look for new ways to incentivize U.S. companies to improve consumer privacy standards without unduly burdening businesses that are victimized by increasingly sophisticated cybersecurity threats.

Finally, the same may be said for the courts, which have begun raising the pleading standard in data breach class action cases to address the increasing number of actions being filed in which no cognizable injury has occurred. Certain courts[10] are requiring plaintiffs to demonstrate actual harm, such as financial loss, identity theft or other tangible damage, rather than merely speculative or hypothetical damage, in cases where personal

information has been compromised. This change reflects a departure from prior case law[11] wherein the potential for identity theft and the mere exposure of personal data were sufficient to establish standing. This heightened standing requirement is reshaping the legal landscape for data breach claims and serves as a counterbalance to the rising tide of consumer protection laws, ensuring that businesses are not unjustly penalized for every potential vulnerability or data exposure and returning the focus to the ways companies can act, or in some cases react, to prevent or mitigate actual harm to consumers.

Takeaway for Companies: The Case for Investing in Cybersecurity

While a company's regulatory obligations may evolve as laws change, one constant is clear: Proactively investing in cybersecurity is always a smart business decision, particularly with the introduction of safe harbor provisions. Although not universal, the trend of courts attempting to limit data breach actions signals a shift in the legal landscape. With legislation and the courts not fully aligned with consumer interests, businesses have an opportunity to improve their standing by demonstrating a commitment to cybersecurity — making a strong case for themselves in the eyes of regulators and the public.

[1] U.S. State Comprehensive Privacy Laws Report, IAPP (October 2024) (available at https://iapp.org/resources/article/us-stateprivacy-laws-overview/?utm_source=Google&utm_medium=Paid&utm_campaign=StatePrivacy&utm_content=&gad_source=1&gclid=CjwKCAiA9IC6BhA3EiwAsbltOFaJudRWwJSBDkJD38JTKfn3Z2ixaVaSTqUtFm37OjALTcwaxxp4phoCpOAQAvD_BwE).

[2] Laura Hopkins et al., Lex Machina Consumer Protection Litigation Report 2024 (July 2024) (available at https://pages.lexmachina.com/2024- Consumer-Protection-Report_LP.html).

[3] Fiscal Note & Local Impact Statement, Ohio Legislative Service Commission (September 2018) (available at https://www.legislature.ohio.gov/download?key=10235).

[4] https://search-prod.lis.state.oh.us/api/v2/general_assembly_132/legislation/sb220/00_IN/pdf/

[5] T.C.A. § 29-34-215(b).

[6] CS/CS/HB 473: Cybersecurity Incident Liability, The Florida Senate (available at https://www.flsenate.gov/Session/Bill/2024/473/?Tab=VoteHistory).

[7] See FL H.B. 473.

[8] R. DeSantis, letter to Sec. of State Byrd (June 26, 2024) (available at https://www.flgov.com/eog/sites/default/files/press/Veto-Letter_HB-473.pdf).

[9] J. Justice, letter to Sec. of State Warner (March 27, 2024) (available at https://www.wvlegislature.gov/Bill_Text_HTML/2024_SESSIONS/RS/veto_messages/HB5338.pdf).

[10] Including federal courts in the 3rd, 4th, 8th and 11th circuits. See Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3rd Cir. 2011); Beck v. McDonald, 848 F.3d 262, 274–75 (4th Cir. 2017); In re SuperValu, Inc., 870 F.3d 763, 770 (8th Cir. 2017); Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1333–24 (11th Cir. 2021).

[11] See Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017); Galaria v. Nationwide

Mut. Ins. Co., 663 F. App'x 384, 387-89 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692, 694-95 (7th Cir. 2015); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142-43 (9th Cir. 2010).