Data Privacy and Cybersecurity - 2023 Year in Review & Looking Ahead to 2024

January 10, 2024

By: Robert Schechter, Alfred Brunetti

Data Privacy

2023 was a remarkably busy year on the national consumer data privacy front and that trend looks sure to continue into 2024. This year, seven states passed comprehensive-style privacy acts into law (DE, IN, IA, MT, OR, TN, TX) and Florida passed its Digital Bill of Rights, which focuses only on the biggest of Big Tech companies, i.e., those with more than $1B in global gross annual revenue. Four of these laws will be in effect by the later part of 2024 (MT, OR, TX and FL) at which point they will join the five state-specific privacy statutes that became fully effective in 2023: CA, CO, CT, VA and (on New Year's Eve) UT.

On December I8, with only a few days left in New Jersey's legislative session, New Jersey's consumer data privacy offering - Senate Bill 332 - received a favorable report from, and was significantly beefed up by, the Assembly Judiciary Committee. Recently proposed amendments would bring SB 332 closer in line to those of the other state laws slated to take effect next year, but only time will tell if it has a chance at passage before the session, and the year, ends at the stroke of midnight.

This year also saw the California Consumer Privacy Act, as amended by the California Privacy Rights Act, uniquely bring employees and job applicants into its scope. In addition, while the California Privacy Protection Agency continues to find its legs, the California AG's Office bolstered its own enforcement of California's privacy regime by conducting investigative sweeps directed toward employee data rights and consumer opt-out of sale requests.

As California's leading efforts on data privacy often have national impact, prudent data privacy practices require monitoring. On the federal side, the FTC has made clear that ensuring the security and proper treatment of sensitive data remains a top priority by obtaining notable settlements against GoodRx, BetterHealth and Vitagene.

Cybersecurity

Under new SEC rules effective as of September 5, 2023, public companies have a duty to report cybersecurity incidents within four business days of determining that an incident was material. The new rules also require, as of December IS, 2023 or June 15, 2024, depending upon the size of the company, that public companies include in their annual reports additional disclosures on cybersecurity incidents and the company's cyber risk management, strategy and governance practices. As these new rules impact publicly traded companies, improved cyber hygiene and practices become a necessity for private business, service providers and professionals that serve larger enterprises in order to remain competitive and meet upstream compliance standards.

In the face of everchanging cyber risk, 2023 brought the signing of a bill into law by Governor Murphy that requires, among other things, "Every public agency and government contractor [to] report cybersecurity incidents to the New Jersey Office of Homeland Security and Preparedness ... within 72 hours of when the public agency or government contractor reasonably

believes that a cybersecurity incident has occurred." N.J.S.A. § 52:17B-I93.3. As such, contractors to public agencies in New Jersey must similarly be mindful of maintaining evolving security standards in and be prepared to timely react to incidents.

An effective first step to understanding your own data privacy and cyber risk profile as we enter 2024 is to assess your sensitive personal and business information, and its availability to others, whether in digital or physical form.

This article originally appeared in the Winter 2024 issue of the Monmouth Memoranda, *the official publication of the Monmouth Bar Association.*