July 18, 2023

A U.S. Data Privacy Law Update: Data Transfers, Delayed CCPA Regulatory Enforcement, and Data Privacy Laws Galore!

by John M. Brigagliano

The pace of privacy developments in 2023 has been breathtaking. Since our recent alert regarding Iowa's comprehensive data privacy law and Colorado's finalized rules, there have been a number of key developments in data privacy law in the U.S. This article provides a high-level overview of these developments. For any specific questions regarding how these developments may impact your organization, please contact us.

E.U.-U.S. Data Privacy Framework Finalized: For those organizations concerned about data transfers from Europe to the U.S., there is finally some relief (although likely only temporary) from the legal uncertainty surrounding such transfers. On July 10, 2023, the European Commission adopted an adequacy decision for the E.U.-U.S. Data Privacy Framework, which entered into force with its adoption. The adequacy decision concluded that the U.S. ensures an adequate level of protection of E.U. personal data for companies participating in the E.U.-U.S. Data Privacy Framework. The European Commission has published a Questions & Answers page regarding the E.U.-U.S. Data Privacy Framework, here. The E.U.-U.S. Data Privacy Framework's website provides information about the new program and a page for self-registration. In the meantime, as the E.U.-U.S. Data Privacy Framework is expected to be reviewed and challenged, companies should continue to implement other tools for data transfers to the U.S., including standard contractual clauses or binding corporate rules.

Colorado and Connecticut Enter into Effect: On July 1, 2023, the Colorado Privacy Act ("CPA") and Connecticut's an Act Concerning Personal Data Privacy and Online Monitoring, went into effect. If either of these laws applies to your organization, it is critical to ensure that your organization's privacy program is up to date. Similar to California, we expect compliance with the CPA to be closely monitored by its applicable regulator. On July 12, 2023, Colorado Attorney General, Phil Weiser, announced that the Colorado Department of Law would begin enforcing the Colorado Privacy Act with a goal of supporting compliance with the law rather than creating challenges for businesses that are complying with the law. Moreover, the CPA's 60-day notice and correction period makes enforcement of the law a relatively cooperative process (at least until the correction period expires on January 1, 2025).

Delayed CCPA Enforcement and Investigative Sweep: On June 30, 2023, a California state court ruled that enforcement of the most recent updates to the California Consumer Privacy Act (as amended by the California Privacy Rights Act) (collectively, "CCPA") regulations could not occur until one year after being finalized. As the

regulations were finalized on March 29, 2023, this delays enforcement of the regulations until March 29, 2024. However, as statutory changes to the CCPA can still be enforced, organizations would be well-suited to proceed with any remaining updates to ensure CCPA compliance. In particular, organizations that are subject to the CCPA and have employees in California may want to consider focusing on their obligations with respect to employees and job applicants. On July 14, 2023, California Attorney General, Rob Bonta, announced an investigative sweep requesting information from certain California employers on CCPA compliance in this area. That enforcement priority is surprising and unwelcome. California regulators themselves discussed at a May 2023 board meeting how the CCPA and its regulations aren't written to address employee data. The regulators recommend future rulemaking on how the law should apply to employee data.

Seven New Comprehensive Data Privacy Laws: Since our last alert, six states have passed comprehensive data privacy laws (Indiana, Montana, Tennessee, Texas, Florida, Oregon) and Delaware currently has a comprehensive data privacy law pending its governor's signature. The general applicability criteria and some key components of these laws are summarized below.

Organizations should determine whether they are subject to these laws and identify key outliers from existing comprehensive data privacy laws to determine what changes are necessary to their privacy programs. Generally, these recent laws follow similar patterns to existing comprehensive data privacy laws in the U.S., including providing privacy notices, granting certain rights to consumers regarding their personal data, responding to opt-out preference signals, conducting data protection impact assessments, entering into certain contractual requirements between controllers and processors, an opt-in or opt-out for the processing of sensitive personal data, and implementing measures to protect personal data. Moreover, such laws generally don't provide consumers with a private right of action.

- **Indiana**: Indiana's SB5, which is effective on January 1, 2026, generally applies to persons that conduct business in Indiana or produces products and services targeted to Indiana residents and that during a calendar year controls or processes the personal data of: (1) at least 100,000 consumers; or (2) at least 25,000 consumers and derives more than 50% of gross revenue from the sale of personal data. SB5 does not impose additional obligations above many of the other comprehensive data privacy laws in the U.S. Therefore, organizations that are subject to such laws should not have to undergo a compliance overhaul to comply with SB5, especially due to its late effective date.
- **Montana**: Montana's Consumer Data Privacy Act ("MCDPA"), which is effective on October 1, 2024, largely aligns with Connecticut. However, notably, the MCDPA's applicability threshold is much lower (perhaps to account for the state's small population). Generally, the MCDA applies to persons conducting business in Montana or producing products or services targeted to Montana residents, and that control or process the personal data of: (1) not less than 50,000 consumers, excluding personal data controlled or processed solely for purposes of completing a payment transaction; or (2) not less than 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data.
- **Tennessee**: The Tennessee Information Protection Act ("TIPA") which is effective on July 1, 2025, introduces a significant outlier to comprehensive data privacy legislation in the U.S. Namely, TIPA provides an affirmative defense to organizations that creates, maintains, and complies with a written privacy policy

that reasonably conforms to the National Institute of Standards and Technology ("NIST") privacy framework. If your organization is already complying with the NIST framework, it is likely that your business is well-situated regarding TIPA compliance. TIPA has a higher applicability threshold than most other U.S. state comprehensive data privacy laws, generally applying to persons conducting business in Tennessee producing products or services that target Tennessee residents and that: (1) exceed $25 million in revenue; and (2) control or process (a) personal information of 25,000 consumers and derive more than 50% of gross revenue from the sale of personal information, or (b) personal information of at least 175,000 consumers during a calendar year.

- **Texas**: The Texas Data Privacy and Security Act ("TDSA"), which is largely effective on July 1, 2024, has unique applicability criteria. Generally, the TDSA applies to persons that: (1) conduct business in Texas or produce products or services consumed by residents of Texas; (2) processes or engages in the sale of personal data; (3) and is not a small business, as defined by the U.S. Small Business Administration ("SBA"). The SBA defines a small business as "an independent business having fewer than 500 employees."[1] Under the TDSA, small businesses must still not engage in the "sale of personal data", defined broadly as the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party.[2] Small businesses should either determine that they are not "selling" personal data or implement a method to obtain the requisite consent. The TDSA also has specific mandatory disclosures for organizations subject to the TDSA that engage in the sale of sensitive personal data or biometric data.
- **Florida**: The Florida Digital Bill of Rights ("FDBR") has certain sections (those regarding data protection impact assessments and prohibiting government-directed moderation of social medial platforms) that were effective as of July 1, 2023. The remainder of the FDBR will be effective on July 1, 2024. The FDBR applies to persons who conduct business in Florida or produce a product or service used by residents of Florida and process or engage in the sale of personal data. However, the FDBR's obligations are inapplicable to many companies since, in order to qualify as a "controller" under the FDBR, a legal entity must make in excess of $1 billion in global gross annual revenues and satisfy one of the following: (1) derive 50% or more of global gross annual revenues from online advertisements; (2) operate a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation; or (3) operate an app store or a digital distribution platform with at least 250,000 different software applications for consumers to download and install.
- **Oregon**: Oregon's SB 619 will largely be effective on July 1, 2024 for for-profit organizations. Although most comprehensive data privacy laws in the U.S. exclude non-profits, for covered non-profit organizations, SB 619 would be effective on July 1, 2025. SB 619 will apply to persons that conduct business in Oregon or that provide products or services to Oregon residents, and that during a calendar year, either: (1) control or process the personal data of 100,000 consumers; or (2) derive 25% of gross annual revenue from the sale of the personal data of 25,000 or more consumers.
- **Delaware**: The Delaware Personal Data Privacy Act ("DPDPA"), which pending action from Delaware's governor, will be effective on January 1, 2025, has lower applicability thresholds than other comprehensive data privacy laws in the U.S. The DPDPA will apply to persons who conduct business in Delaware or provide products or services to Delaware residents, and that during a calendar year, either: (1) control or

process personal data of 35,000 consumers, excluding personal data controlled or processed for the purpose of completing a payment transaction; or (2) control or process the personal data of 10,000 consumers and derive more than 20% of gross revenue from the sale of personal data.

Washington, Nevada, and Connecticut Regulate Consumer Health Data: Separate from comprehensive data privacy laws, Washington and Nevada have passed laws regulating consumer health data. In addition, Connecticut made amendments to its comprehensive data privacy law to regulate consumer health data. To understand more about these important laws (which include a private right of action in Washington), please see the "Legislative Controls" section in this article, and over the next several weeks, we plan to publish more on this topic.

Last but not least, please stayed tuned for our team's deep dive into key compliance requirements of comprehensive data privacy laws in the U.S., which are designed to help make your life as an in-house counsel or a privacy professional a little bit easier.

Special thanks to Maya Langendoen for her contributions to this article.

Footnotes

---

[1] SB-FAQ-2016_WEB.pdf (sba.gov)

[2] "Sale" has been broadly interpreted under the CCPA by the California Attorney General to include certain online tracking. For more, see this article.