Riding the Wave of New Data Privacy and Security Laws in 2023

By Anna Mercado Clark and Jeffrey D. Coren
Phillips Lytle LLP

This year has seen a surge of new U.S. data privacy and security laws at the federal, state and local levels. Five comprehensive state data privacy laws take effect in 2023, and four other states have enacted or passed their own comprehensive data privacy laws over the last several months. At the same time, federal and state agencies have proposed sweeping new data security regulations.

Anna Mercado Clark
Partner

Jeffrey D. Coren
Special Counsel

Comprehensive State Data Privacy Laws

Five comprehensive state data privacy statutes have taken effect in 2023 or will become effective later this year: California (effective January 1, 2023); Virginia (effective January 1, 2023); Colorado (effective July 1, 2023); Connecticut (effective July 1, 2023); and Utah (effective December 31, 2023).

Three other states have enacted comprehensive data privacy laws in the past several months: Iowa (enacted March 28, 2023; effective January 1, 2025); Indiana (enacted May 1, 2023; effective January 1, 2026); and Tennessee (enacted May 11, 2023; effective July 1, 2025). Montana is poised to become the ninth state with a comprehensive data privacy law, with its legislature having passed a data privacy statute in April 2023 that is awaiting approval by the governor. Other states may soon follow suit.

Common consumer rights in these comprehensive privacy laws include data access, data portability, data deletion, data correction and opt-out rights regarding data sales, advertising or profiling. Common business or controller obligations include data processing restrictions (such as notice or consent), consent related to children's data, privacy notices, data security requirements, assessments, prohibiting discrimination for exercising data rights and requirements for responding to consumer requests.

Although similar, these laws have nuanced requirements and even different thresholds for applicability. Applicability is largely based on annual revenue, consumer data volume, data sale activity and a company's business activities in the state or directed at consumers in the state. Each law may also have different compliance requirements and limited exemptions, such as for certain federally regulated entities and/or data. Notably, these laws may apply to businesses located inside and outside the state. For example, the Virginia law may apply to a company that conducts business in the state or produces products or services targeted to Virginia residents if it meets certain data processing or sale thresholds. The Utah law, on the other hand, has an annual minimum revenue threshold of $25 million in addition to certain data processing or sale thresholds.

Proposed Cybersecurity Regulations

On November 9, 2022, the New York State Department of Financial Services released proposed amendments to its cybersecurity regulations for financial services companies. If adopted, some of the proposed amendments could take effect within 180 days.

On March 15, 2023, the U.S. Securities and Exchange Commission proposed new cybersecurity rules that would apply to a broad range of market participants that include certain broker-dealers, clearing agencies, security-based swap participants, national securities associations and national securities exchanges. New requirements may include certain written policies and procedures, annual reviews, cybersecurity event reporting and recordkeeping. Proposed cybersecurity rules for investment advisers and investment companies are also pending.

An Eye Toward the Future

Businesses should be mindful of the constantly evolving landscape of data security and privacy, and examine whether their existing policies, procedures, vendor contracts and data security posture comply with existing, as well as new and emerging, laws and regulations.

Anna Mercado Clark, CIPP/E, CIPP/US, CIPM, FIP, is a partner at Phillips Lytle LLP and leader of the firm's Data Security & Privacy and E-Discovery & Digital Forensics Practice Teams. She can be reached at aclark@phillipslytle.com or (716) 847-8400 ext. 6466.

Jeffrey D. Coren is special counsel at Phillips Lytle LLP and a member of the firm's Data Security & Privacy Practice Team. He can be reached at jcoren@phillipslytle.com or (716) 847-7024.