New Data Privacy and Cybersecurity Developments That Could Impact Your Business

By Anna Mercado Clark
Phillips Lytle LLP

Protecting consumer and employee privacy continues to be a priority for states and the federal government and so too should businesses. New state data protection laws and evolving federal regulations impose or enhance businesses' data protection obligations, and carry fines and penalties for failure to comply.

Anna Mercado Clark
Partner

Among recent developments, New York businesses should pay particular attention to the following:

- Passage of two new comprehensive state consumer privacy laws that will take effect in 2023, joining other state laws which will also be amended or take effect in 2023.
- A recent New York law amendment requiring notice of electronic employee monitoring.
- The Federal Trade Commission's (FTC) updated Safeguards Rule that clarifies how financial institutions may comply with their obligation to safeguard consumer information.

State Consumer Privacy Laws

Utah and Connecticut became the latest states to pass comprehensive consumer privacy legislation. California, Colorado and Virginia previously passed similar laws. Although these laws differ in a number of respects, in general, they set forth a framework for processing personal data, define the obligations and standards for companies that control or process personal data, and enumerate individual consumer rights regarding their own data.

The California law will be amended, and the other four laws will go into effect, in 2023. To prepare, businesses should, among other things:

- Determine which of these laws apply.
- Establish or evaluate existing cybersecurity safeguards.
- Create/update the process to respond to requests for consumer personal data.
- Review/update their privacy policy.
- Review/update third-party contracts.
- Determine when data processing requires informed consent or consumer opt-out.

Notably, these out-of-state laws may apply to New York businesses regardless of whether they have a physical presence in those states.

New York Employers Must Provide Notice of Electronic Monitoring

The New York Civil Rights Law was amended in May 2022 to require most New York employers to provide notice if they monitor or otherwise intercept employees' telephone or electronic communications or transmissions, internet access or usage of or by an employee of electronic devices or systems. Such notice must be provided in advance and acknowledged in writing by new employees upon hiring. Current employees are to be informed through conspicuous postings in the workplace.

The FTC's Final Rule Amends the Safeguards Rule of the GLBA

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions — companies that offer consumers financial products or services like loans, financial advice or insurance — to safeguard sensitive data. The FTC, which enforces GLBA, recently updated its accompanying Safeguards Rule to expand and clarify GLBA data security requirements.

As a result, effective January 2022 (with some requirements taking effect later in the year):

- Non-banking financial institutions must comply with the Safeguards Rule (e.g., mortgage brokers, motor vehicle dealers, etc.), with some institutions exempt from certain requirements if they collect relatively less information.
- Standards and more specific guidance regarding security programs take effect.
- There is an increased focus on internal accountability, such as through the designation of a qualified individual to oversee the security program and required periodic reporting to senior management.

It can be extremely challenging to assess and update your business's privacy and security posture given the complex overlay of state laws and federal regulations in this area. In most cases, a compliance assessment involves a multi-step analysis.

Phillips Lytle is uniquely situated to provide legal advice and services in the data security and privacy areas due to the technical backgrounds of our practice area partners and decades of successful representation of businesses and financial institutions in data crisis planning and security breaches.

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.