ECKERT SEAMANS ATTORNEYS AT LAW

December 2021

Data Security & Privacy Alert

Cybersecurity and Privacy: What Companies Need to Know for 2022

By Sandy B. Garfinkel, Stephenie Scialabba and Emma Lombard

As 2021 comes to a close, there are a large number of critical data security and privacy legal developments for companies to be aware of in the coming year, including: (a) laws that have been enacted and will soon become effective; (b) laws now being considered for enactment; and, (c) rules/regulations on privacy and security.

State Consumer Privacy Laws Going Into Effect in 2023

These bills generally incorporate the basic concepts regarding access, notice, restrictions on the sale of information, and affirmative rights for consumers that originated with the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act ("CCPA"). Still, there are key differences and, in some cases, added compliance burdens and risks to companies.

California Privacy Rights Act ("CPRA") (see previous CCPA alert here and here)

- Effective December 16, 2020, but most provisions revising CCPA become "operative" January 1, 2023
- Expands existing consumer rights and creates four new consumer rights, among others
- Creates a new class of vendors and contractors with associated obligations
- Establishes the California Privacy Protection Agency with investigatory, enforcement, and rulemaking authority

Virginia Consumer Data Protection Act ("VCDPA")

- Effective January 1, 2023
- Includes a "look back" period for data collected during the final months of 2022
- Differs from CCPA/CPRA in that it lacks a standalone revenue threshold and expressly excludes persons acting in commercial or employment context from "consumers"

Colorado Privacy Act ("CPA")

- Effective July 1, 2023
- Definition of sale includes an exchange for monetary or "other valuable" consideration

The "Big Three" State Privacy/Cybersecurity Bills

New York, New Jersey, and Massachusetts are each eyeing legislation that will bring a new twist on U.S. state comprehensive privacy/security laws. Like those addressed above, these bills incorporate now-familiar concepts while imposing new obligations, including fiduciary duties and impact assessments for automated decision-making. Similar legislation is being considered in Minnesota, North Carolina, Pennsylvania, and Ohio.

(1) New York Privacy Act (NYPA – S. 6701)

- Scope: covers all companies that process personal data of NY residents
- Creates fiduciary duties of care, loyalty, and confidentiality
- Private right of action for any violations of consumer rights

(2) New Jersey Disclosure and Accountability Transparency Act (NJ DaTA – A. 3283)

- Scope: covers "controllers and processors" of personally identifiable information
- Establishes the Office of Data Protection and Responsible Use in Division of Consumer Affairs with investigatory, rulemaking, and regulatory authority

(3) Massachusetts Information Privacy Act (MIPA – S.46)

- Scope: covers businesses operating in MA, subject to revenue and quantitative information collection thresholds
- Covered transactions are broadly defined and include mere offers of products/services, targeted advertisements, and creation of an account
- Establishes the Massachusetts Information Privacy Commission, with enforcement, investigation, rulemaking and regulatory authority
- Private Right of Action for any violations of MIPA

Security Rules / Regulations

Banking Cybersecurity Rules. On November 18, 2021, the federal banking agencies (FDIC, FRB, and OCC) issued computer security incident rules that require a "banking organization" to notify its primary federal regulator of a covered security incident within 36 hours of occurrence. Beginning May 1, 2022, a "computer security incident" requires notification if it has or is likely to materially disrupt or degrade a banking organization's ability to carry out banking operations or provide services to customers.

Transportation Cybersecurity Directives. On December 2, 2021, the Transportation Security Administration ("TSA") issued two emergency security directives that impose obligations on freight railroad carriers and owner/operators of passenger railroad carriers or rail transit systems.

They become effective December 31, 2021, and require four critical actions:

1. Designate Cybersecurity Coordinator at the corporate level who is available 24/7 to TSA and CISA within seven days
2. Report cybersecurity incidents to CISA within 24 hours of occurrence

3. Develop a Cybersecurity Incident Response Plan within 180 days
4. Conduct a cybersecurity vulnerability assessment and submit it to TSA within 90 days

TSA also recently updated its aviation security programs to require airport and airline operators to implement the first two provisions above.

Conclusion

There is a marked acceleration toward the development of state consumer privacy laws and a tightening of regulatory cybersecurity mandates. Together, these trends will present significant compliance challenges for industries and companies during 2022.

ECKERT SEAMANS ATTORNEYS AT LAW