SpencerFane®

The Data Breach Tide is Shifting Toward Proactive Security Obligations

JULY 13, 2018| PUBLICATIONS

AUTHORS

- Stacy Harper
- Thomas W. Hayde, CIPP/US

RELATED PRACTICES

- Data Privacy and Cybersecurity

When an organization faces a security incident, it is thrown into a complicated analysis of forty-seven state breach notification laws. With the laws based on the residence of the affected consumer, consideration must be given to the variances in the definition of a breach that triggers notification; the content, timing, and manner of notification; additional regulatory, credit agency, or media communications; and potential litigation or enforcement. Thus, the states in which an organization provides goods or services and collects personal information can have a significant impact on obligations following a security incident.

Recent amendments to the data laws in some states are expanding this impact to create pre-incident obligations. Alabama became the 50th and final state in the union to adopt a data breach notification law, which went into effect June 1, 2018. The law provides a broader definition of covered personal information than most other states, with the inclusion of both health and health insurance related information, as well as an e-mail address together with a password that would allow access to an online account. Alabama also joined a minority of state laws that explicitly require business to implement and maintain reasonable information security measures, including to require all data-handling vendors to meet those same requirements. Another notable feature of the Alabama law is that it only requires consumer notification where there is a risk of "substantial" harm to the consumer. Delaware amended its breach notification law effective in April 2018 to expand the definition of personal information, require credit monitoring and attorney general notification in some situations, and require all persons who conduct business in the state to implement reasonable procedures and practices to prevent unauthorized acquisition, use, modification, disclosure or destruction of personal information.

Colorado's amendments to its consumer data law go into effect on September 1, 2018. The Colorado law not only requires breach notification to be provided within thirty days and expressly overrides the sixty day notification timeline under HIPAA, but also requires organizations that maintain, own or license personal identifying information of Colorado residents in the course of business to implement certain data destruction requirements, use reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business, and impose similar requirements on third-party vendors.

Of most significance is the California Consumer Privacy Act of 2018 ("CCPA") which represents a sea change in American approaches to privacy. Much like the European Union's General Data Protection Regulation ("GDPR") that went into effect in May 2018, the CCPA treats individuals as having fundamental rights in all nonpublic information concerning them . Like the GDPR, the CCPA defines "personal information" very broadly – literally any nonpublic information about an individual. Personal information is any "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Also similar to the GDPR, the CCPA provides California consumers with substantial rights concerning their information, and requires that businesses that collect, sell or disclose their information to implement compliant policies and procedures by January 1, 2020.

The consumer privacy rights afforded by the CCPA include:

- The right to request and receive a disclosure of what information a business collects, sells or discloses about them, where the business gets the information, and the business purpose for collecting it;
- The right to obtain a copy of the personal information a business has about them, including in a format that is easily readable and can readily be ported to another service provider;
- The right to have a business delete their personal information (subject to certain exceptions);
- The right to object and opt out of the sale of their information;

- The right not to be discriminated against for exercising their privacy rights, and to receive services on equal terms and pricing

In addition, the CCPA requires businesses to update their privacy notices to reflect CCPA rights and requirements.

The CCPA provides exceptions to information that is subject to HIPAA, California Confidentiality of Medical Information Act, Gramm Leach Bliley, and other limited situations, such as when every aspect of the commercial conduct takes place outside of California.

The CCPA provides for enforcement by the California Attorney General, with fines of up to $2500 per incident per consumer for failure to cure violations within 30 days, and fines of up to $7500 per incident per consumer in cases of intentional violations.

In the event of an unauthorized access, exfiltration, theft or disclosure of personal information based on the business's failure to maintain reasonable security procedures, the CCPA also provides consumers with the possibility of a private right of action, with statutory damages of $100-$750 per consumer per incident or actual damages, whichever is greater, injunctive relief, or any other relief as the court deems proper. Consumer claims for statutory damages only are subject first to a 30 day notice and cure period, and then another 30 day notice period for the state attorney general to decide whether to prosecute or allow the consumer the right to sue. Consumer claims for actual damages are not subject to those prerequisites.

The latest wave of state data laws may indicate a shift in the focus from timely response to a security incident to the implementation of practices and procedures to prevent the incident in the first place. The new California law will apply to any business serving California consumers, and may portend a broader American shift towards the EU approach to treat all citizens as having a fundamental privacy right in all nonpublic information concerning them. In order to survive the evolving expectations, all organizations, especially those that conduct business in multiple states, will need to continually assess 1) the types of personal information collected and maintained; 2) the flow of that information in, out and through the organization; and 3) the systems and processes in place to protect and maintain the information.

This post was drafted by Spencer Fane LLP attorneys Stacy Harper in the Overland Park, KS office, and Thomas Hayde in the St. Louis, MO office. For more information, visit spencerfane.com.