Chicago Daily Law Bulletin®

Serving the profession since 1854

August 24, 2020

The coasts are alive with the sound of privacy enforcement

By Daniel A. Cotter
Daniel A. Cotter is a partner at Howard & Howard Attorneys PLLC and author of the book "The Chief Justices" (Twelve Tables Press). The views expressed here are solely those of the author. He can be reached at scotuslyyours@gmail.com.

Last week, we reviewed the invalidation of the Privacy Shield. This week, we continue to review cyber and privacy developments, this week directly on a few developments in the United States.

The California Consumer Privacy Act

In June 2018, California's governor signed legislation that the California legislature passed, the California Consumer Privacy Act (the "CCPA"). The CCPA provided new privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.

When enacted, the act was referred to as the "toughest online privacy law" and the most "sweeping data privacy bill" and was compared to the EU General Data Protection Regulation.

On August 14, the California Office of Administrative Law approved and released the Final Regulations for the CCPA. Before the Final Regulations were approved, the California Attorney General had already started to take enforcement steps against companies, sending out notices of noncompliance.

While the CCPA set forth the steps and procedures companies holding consumers' information must take, the Final Regulations set forth in the 28 pages what steps companies should take to comply. These steps include:

• Reviewing and updating privacy policy disclosures. All policies should be reviewed and update to disclose additional data privacy collection, use, disclosure and sale practices, and provide details on the business's verification and processing of requests, and financial incentives the business provides.

• Providing updated notice of collection of personal information. Provide timely notice of collection and use of personal information to employees and consumers online, in-store and via mobile applications, and update that notice as collection practices change. (This is also a focus of Federal Trade Commission enforcement actions in recent years, with significant penalties assessed on those businesses that have practices different from those disclosed.)

• Reviewing and adjusting methods for Accepting and Responding to Consumer Requests. Ensure consistency with CCPA requirements, including, for example, ensuring that sensitive personal
information (i.e., SSNs, account passwords, biometric information, etc.) is never disclosed.

• Applying reasonable security controls to responses to consumer requests. Specific security controls and measures are necessary to ensure that personal information provided to a consumer pursuant to a consumer request is subject to reasonable security procedures.

• Adhering to guidelines for verifying consumer requests. The Final Regulations provide guidelines for verifying consumer requests for general as well as specific information.

• Establishing adequate recordkeeping. Businesses must maintain records of CCPA consumer requests in a specific form for at least 24 months.

• Enabling notice to individuals with disabilities. The Final Regulations address ensuring that the required notices regarding the business's privacy practices is reasonably accessible to consumers with disabilities.

• Confirming receipt of consumer requests. Consistent with the CCPA, the Final Regulations require that businesses must respond to consumer requests within ten days of receipt, informing the consumer of the business's verification process and timing for response. Given the AG's recent activity, this likely will be closely monitored by California.

The CCPA and Final Regulations set forth onerous obligations on companies who do business with California consumers. Anyone doing business in California should closely review the Final Regulations and seek guidance if questions arise. As noted, the California attorney general is busy addressing issues of noncompliance and more is likely to follow.

East Coast privacy enforcement

On March 1, 2017, 23 NYCRR 500 became effective.

Under the New York Cybersecurity regulation, "operating under a license, registration, charter, certificate, permit, accreditation or similar authorization under" the banking law, insurance law, or financial services law of the State of New York. Until recently, no known enforcement action had been initiated by New York pursuant to 23 NYCRR 500. That all changed on July 21, 2020, when the New York Department of Financial Services ("NYDFS") filed an action against First American Title Insurance Company. According to the statement of charges:

"From at least October 2014 through May 2019, due to a known vulnerability on Respondent's public-facing website (the "Vulnerability"), these records were available to anyone with a web browser."

The charges allege that even after learning of the Vulnerability in 2018, First American did not remediate it for a period of time. The charges detail the reporting of a journalist, Brian Krebs, who wrote that First American "had exposed 885 million documents — dating as far back as 2003 and many containing NPI — by rendering the documents openly accessible to the public." After reciting the various facts and analyzing them, the NYDFS charged First American with violations of: 1) 23 NYCRR 500.02 (maintenance of cybersecurity program), 2) 23 NYCRR 500.03 (written policy or policies), 3) 23 NYCRR 500.07 (limit user access privileges), 4) 23 NYCRR 500.09 (periodic risk assessment), 5) 23 NYCRR 500.14(b) (cybersecurity awareness training), and 6) 23 NYCRR 500.15 (implantation of controls, including encryption).

Those in the impacted industries in New York, and in other jurisdictions, especially insurers who have versions of the NAIC cybersecurity model law to comply with, will be watching this action closely. The NYDFS often has been a leader in development of enforcement laws that have spread to other states in the nation. Businesses who fall under the oversight of the NYDFS should review their cyber policies and practices to ensure they are in good shape in light of the regulations that have been in place for more than three years and have begun to be enforced by the NYDFS.

Conclusion

Recent activity in the cyber and privacy arenas suggest that all companies regardless of industry should review their privacy practices and their online privacy disclosures and security procedures to ensure they follow myriad laws in place that impact them. Fail to do so might find adverse consequences not just on the coasts, but in all jurisdictions as they revisit privacy and data security.
