THOMSON REUTERS
Westlaw®

Nevada adds 'do not sell' requirement to privacy law

By Shea M. Leitch, Esq., and Alan L. Friel, Esq., *BakerHostetler**

JUNE 19, 2019

On May 29, Nevada Governor Steve Sisolak signed new privacy legislation into law in Nevada. Senate Bill 220[1] (SB-220) updates Nevada Revised State 603A to provide consumers a new right to opt out of the sale of their data.

Effective Oct. 1, 2019, the new law will come into effect prior to the more comprehensive California Consumer Privacy Act[2] (CCPA). Accordingly, the Nevada law will be the first law in the United States granting consumers the right to opt out of data sales.

CONSUMER RIGHTS

The rights provided in SB-220 are far more circumscribed than those set forth in the CCPA or the European Union's General Data Protection Regulation[3] (GDPR). Whereas the CCPA and GDPR provide broad rights to access and/or portability and deletion, SB-220 provides consumers only the right to opt out of data sales.

Also, unlike the current version of the CCPA, which broadly defined "consumers" as state taxpayers (a pending bill may change that), "consumer" is defined as a "person who seeks or acquires, by purchase or lease, any good, service, money or credit for personal, family or household purposes from the Internet website or online service of an operator." Thus, employees and business-to-business contacts are excluded from the definition of "consumer" under SB-220.

Under SB-220, consumers will have the right to direct website operators not to sell certain information. SB-220 defines "sale" as "the exchange of covered information for monetary consideration by the operator to a person for the person to license or sell the covered information to additional persons."

"Covered information" means name, physical address, email address, phone number, Social Security number, "[a]n identifier that allows a specific person to be contacted either physically or online" and "[a]ny other information concerning a person collected from the person through the Internet website or online service ... in combination with an identifier in a form that makes the information personally identifiable."

Once effective, SB-220 will extend to consumers the broad right to direct companies processing their data not to sell that data. The bill excludes from the definition of "sale" the transfer of data to service providers that process data on behalf of the website operator that collects the data from the consumer.

Disclosures for purposes of providing a product or service at the request of the consumer are also excluded, as long as the consumer has a direct relationship with the entity to which the data is disclosed.

Notably, data disclosures "consistent with the reasonable expectations of a consumer considering the context in which the consumer provided the covered information" are excluded from the definition of "sale." This language will give companies some wiggle room to disclose data to third parties, as long as those disclosures are within the "reasonable expectations of [the] consumer."

Conceivably, transfers for purposes about which consumers are notified in a website privacy policy could be within the "reasonable expectations of a consumer" in the context of an online transaction. Thus, the Nevada legislation appears to provide companies flexibility to structure transactions in a manner that would not be considered "sales" under SB-220.

Under SB-220, companies must provide a "designated request address" through which consumers may submit requests. Unlike the CCPA, which explicitly requires companies to accept requests via both a toll-free phone number and website (at a minimum, and again, a pending bill may change that), the Nevada legislation will permit companies to choose to accept requests via email, phone or website.

Companies will have 60 days to respond to do-not-sell requests, with the option to extend the deadline by an additional 30 days where the extension is "reasonably necessary" and with notice of the extension to the consumer.

GLBA AND HIPAA CARVE-OUTS

SB-220 updates the current definition of "operator" to exclude GLBA- and HIPAA-covered entities. As a result, organizations subject to GLBA and HIPAA will not only be exempt from the consumer rights requirements of SB-220, but once SB-220 is effective, they will no longer be required to comply with Nevada's existing notice requirements, which are discussed below.

NOTICE REQUIREMENTS

Unlike the CCPA and the GDPR, SB-220 does not add new notice requirements for website operators. Rather, existing requirements for notice to Nevada consumers are maintained. Under existing law, which was modeled after California's Online Privacy Protection Act (CA OPPA), companies must provide the following information in their website privacy policy:

- Categories of information collected.
- Categories of third parties with which the data is shared.
- A description of the process consumers may use to review and request changes to their covered information (if a process for doing so exists).
- A disclosure that third parties may track the consumer's online activities "over time and across different Internet websites" (if applicable).
- The "notice effective" date.

ENFORCEMENT AUTHORITY

Under existing Nevada law, the attorney general has exclusive enforcement authority for violations of Nevada's privacy and security requirements set forth in NRS 603A et seq. SB-220 maintains this arrangement, providing no express private right of action to consumers.

Organizations that violate any of the privacy and security requirements may be subject to a penalty up to $5,000 per violation and a temporary or permanent injunction after being provided notice of the violation and an opportunity to cure by the Nevada attorney general.

CONCLUSION

Though privacy legislation has stalled or failed in other states, Nevada's passage of SB-220 serves as a reminder that maintaining compliance with legal and regulatory obligations in a digital world will remain a challenge in the near future. We are watching several other states where CCPA-inspired legislation is still under consideration.[4]

In light of this shifting legal landscape, it is critical for organizations to have a good handle on all their data processing operations and the third parties to whom data is transferred. By doing so, organizations can position themselves to ensure that they can meet new legal demands as they arise.

For more information on how to prepare for CCPA and potential other new U.S. privacy laws, see our U.S. Consumer Privacy Resource Center[5] or contact the authors.

NOTES

[1] https://bit.ly/2I8YjNZ

[2] https://bit.ly/2XCyPy1

[3] https://bit.ly/2WzF4Gh

[4] For an update on California bills proposing to amend CCPA, see https://bit.ly/2IEbTYD.

[5] https://bit.ly/2G3kYcb

This article first appeared on the Practitioner Insights Commentaries web page on JUNE 19, 2019.

ABOUT THE AUTHORS

Shea Leitch is a Seattle-based associate on the Privacy and Data Protection team at BakerHostetler. With CIPP/US and CIPP/E certifications from the International Association of Privacy Professionals, Leitch serves clients in an array of industries and provides counsel on everything from the development of enterprise-wide privacy and security compliance programs to targeted guidance on discrete privacy and security issues. **Alan L. Friel** is a partner working out of the firm's offices in Los Angeles and Costa Mesa, California. A member of the firm's Advertising, Marketing and Digital Media and Privacy and Data Protection teams, he focuses his practice on intellectual property transactions, regulatory schemes, and privacy and consumer protection law. Friel also coordinates the firm's Retail and e-Commerce industry initiative and co-leads the firm's U.S. Consumer Privacy practice that counsels clients on compliance with the new California Consumer Privacy Act and other data privacy regimes. This article was first published June 5, 2019, on the firm's Data Privacy Monitor blog. Republished with permission.