Nevada and Maine Advance Legislation Addressing the "Sale" of Personal Data

June 4, 2019

While businesses rightfully have been focused on preparing for the California Consumer Privacy Act ("CCPA"), the Nevada and Maine Legislatures have moved forward with legislation that, like the CCPA, features new requirements relating to the sale of consumer personal data. The Nevada bill, which was signed into law on May 29 and amends an existing data privacy statute, requires companies to provide a designated channel through which consumers can opt out of the sale of their personal data. The Maine bill, which has passed house and senate votes, notably would require *opt-in* consent prior to the sale of personal data; however, the law would narrowly apply to Internet Service Providers ("ISPs") and exclude online companies perhaps more commonly associated with the disclosure and sale of consumer data.

- **Nevada**

Nevada's SB 220 amends the state's existing online privacy notice statute, NRS 603A.300 to .360, to add a provision that requires "operators" – which include *most* companies that conduct business online with Nevada residents – to comply with a consumer's do-not-sell request (health care and financial institutions subject to HIPAA and GLBA are out of scope of the law). As of the October 1, 2019 effective date, operators are required to create a "designated request address," such as an email address, toll-free number, or website, through which consumers can submit a "verified request" to restrict the sale of covered data. A "verified request" is one where the operator can reasonably verify the authenticity of the request and the consumer's identity using "commercially reasonable means," which the law does not define.

The personal information covered under the law includes personal data such as name, address, and SSN, as well as online contact information, and any other data collected by the company that could be viewed as personally identifiable. Notably, the law defines "sale" more narrowly than the CCPA to include the exchange of covered information for "monetary consideration" to a person "for the person to license or sell the covered information to additional persons."

Operators will have 60 days to respond to a consumer's do-not-sell request, though this timeline may be extended by up to 30 days where the operator deems it necessary and notifies the consumer. The provision will be enforced by the Nevada Attorney General's Office, which can impose a penalty of up to $5,000 per violation.

- **Maine**

The bill advanced by the Maine Legislature, titled "*an Act to Protect the Privacy of Online Customer Information*," would among other things prohibit ISPs' use, disclosure, and sale of "customer personal information" without a customer's opt-in consent, except under limited circumstances such as to provide the requested service, to collect payment, and several other narrow scenarios.

Customer personal information subject to the law broadly would include (1) personally identifiable information about an ISP customer; and (2) information relating to a customer's use of broadband Internet access service, including web browsing history, app usage, device identifiers, geolocation data, and other usage information. ISPs also would be prohibited from making the sale of data mandatory under the applicable terms of service, or refusing service to customers who do not consent to data collection.

The bill is an attempt to restore at the state level core provisions within the FCC's 2016 broadband order that were repealed by Congress in 2017. The Maine State Chamber of Commerce has opposed the bill, claiming that ISPs are being unfairly singled out, and arguing that the law would result in a false sense of privacy for consumers given that large web-based companies such Facebook and Google would not be subject to the law. The Governor still must sign the final legislation, which would take effect July 1, 2020.