Nevada and Maine Impose New Data Privacy Protections

June 17, 2019

States continue to fill the data privacy legislative vacuum created by Congressional inaction. Nevada and Maine recently enacted new consumer data protection laws. Neither is as sweeping as the California Consumer Privacy Act (CCPA), but both offer similar, and sometimes stronger, privacy protections.

Nevada

Nevada's amended "Security and Privacy of Personal Information" law (SPPI) goes into effect October 1, 2019. Like California's CCPA, it will give consumers the right to opt out of the sale of their personal information.

Rather than force a website to place a conspicuous "Do Not Sell My Personal Information" button on a website, as the CCPA does, Nevada requires websites to create a "designated request address" for Nevada consumers to send a "no sale" directive regarding their data.

If a site operator fails to adhere to a consumer's verified request within 60 days (plus one 30-day extension), the Nevada Attorney General can seek fines of up to $5,000 per violation. The SPPI does not allow private causes of action.

Nevada limits its definition of "sale" to exchanges of personal information for money, compared to California's broad definition that includes an exchange of personal information for anything of value.

The SPPI already applies to website owners or operators of commercial websites directed to Nevada and that collect "covered information" from Nevada consumers. It does not apply to financial institutions under GLBA or covered entities under HIPAA.

Websites must notify consumers of the categories of covered information collected, with whom it is shared, the process for reviewing and correcting it, any third party collection via the site, and changes to the entities' privacy policies.

Maine

Maine's new Broadband Internet Access Service Customer Privacy Act is set to take effect on July 1, 2020. The act prohibits internet companies from selling consumer real-time location data and internet and cable usage data to third parties.

The FCC used to enforce such prohibitions against both cable and internet companies until President Trump nullified the practice in 2017. Maine's new law has reimposed the restriction to protect internet users.

An internet provider must receive affirmative customer consent before it can use, disclose, sell, or permit access to customer "personal information," defined broadly to include items such as browsing history, application usage, geolocation, financial or health information, information about children, and IP address.

Maine's approach illustrates the difference between opt-in and opt-out consent. Maine customers must affirmatively agree to the use of their personal information, while California's CCPA requires that a consumer click a website button to opt out - otherwise, silence or inaction means the use is permitted.

Maine is likely not done with consumer data privacy protections. The sponsor of the Broadband Internet Access Service Customer Privacy Act is promising broader consumer protections in Maine's next legislative session.

The landscape of privacy and data security legislation is changing rapidly. If you need assistance in keeping abreast of the latest in this fast-paced area of law, let Lathrop Gage's Cybersecurity and Data Privacy department make sure that you stay ahead of the law.