BLANKROME

Cybersecurity & Data Privacy

AUGUST 2019 • NO.1

Nevada Adds New Opt-Out Right to State Consumer Privacy Law

Nevada has followed in the footsteps of California and its enactment of the game-changing California Consumer Privacy Act of 2018 ("CCPA") with a significant enhancement to the state's own consumer privacy law. Known as Senate Bill 220 ("SB-220"), the new law grants consumers the right to opt out of the sale of their personal information. Importantly, Nevada's new opt-out requirement will go into effect on October 1, 2019. As such, companies will have to take action quickly to get in compliance with the new law before the opt-out requirement goes into effect in less than two months.

SB-220 & NEW OPT-OUT RIGHT

SB-220 amends the state's online privacy policy law to add a new right for "consumers" to direct an operator to not make any "sale" of "covered information" that the operator has collected or will collect on the consumer. Once an operator receives an opt-out request, it is prohibited from selling any covered information that the entity has collected or collects in the future with respect to the requesting consumer.

In addition, SB-220 also requires operators to establish a designated request address for consumers to submit opt-out requests. The designated request addresses can be in the form of an e-mail address, toll-free telephone number, or website.

Finally, SB-220 also mandates that operators respond to "verified" opt-out requests within 60 days of the submission of a request. Covered entities can extend the deadline by another 30 days where the extension is "reasonably necessary" and notice of the extension is provided to the consumer. The term "verified request" is defined as one for which "an operator can reasonably verify the authenticity of the request and the identity of the consumer using commercially reasonable means." However, SB-220 does not define what qualifies as "commercial reasonable means."

The term "operator" is defined broadly in SB-220 to include any entity that: (1) owns or operates an Internet website or online service for commercial purposes; (2) collects and maintains covered information from consumers who reside in Nevada and use or visit the Internet website or online service; and (3) purposefully directs its activities toward Nevada, consummates some transaction with Nevada or a resident thereof, purposefully avails itself of the privilege of conducting

activities in Nevada, or otherwise engages in any activity that constitutes sufficient nexus with Nevada to satisfy the requirements of the United States Constitution. Significantly, SB-220 updates the definition of "operator" to exclude both financial institutions subject to the Gramm-Leach-Bliley Act ("GLBA"), as well as health care institutions subject to Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Consequently, entities subject to GLBA or HIPAA are not only afforded an exemption from the opt-out requirement of SB-220, but Nevada's consumer privacy law as a whole, with SB-220 negating the responsibility of those entities to adhere to the law's previously-enacted notice requirements as well.

The term "covered information" remains unchanged from Nevada's original privacy law, and entails: (1) a first and last name; (2) a home or other physical address that includes the name of a street and the name of a city or town; (3) an e-mail address; (4) a telephone number; (5) a Social Security number; (6) an identifier that allows a specific person to be contacted either physically or online; or (7) any other information concerning a person collected from the person through a website or online service of the operator and maintained by the operator in combination with an identifier in a form that makes the information personally identifiable.

Likewise, the term "consumer" also remains unchanged from Nevada's original privacy law, and is defined as any individual who "seeks or acquires, by purchase or lease, any good, service, money, or credit for personal, family, or household purposes."

The term "sale" is defined in SB-220 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." Excluded from the definition of "sale" is the transfer of data to service providers that process data on behalf of the operator that collects the data from the consumer. In addition, disclosures of data "consistent with the reasonable expectations of a consumer considering the context in which the consumer provided the covered information" are also excluded from the definition of "sale" as well. Unlike the definition of "sale" under California's CCPA, under the Nevada law a "sale" is limited to what a lay person might consider a sale.

Enforcement of SB-220 (and the state's previously-enacted privacy notice requirements) rests exclusively with Nevada's attorney general. Covered businesses can breathe a sigh of relief, as the new law expressly states that it does not provide a private right of action for consumers to pursue litigation for violations of either facet of Nevada's online privacy law. Covered organizations that are found to have violated the state's notice or opt-out requirements may be subject to civil penalties of up to $5,000 per violation, as well as a temporary or permanent injunction, after receiving notice of the violation and an opportunity to cure by Nevada's attorney general.

COMPLIANCE TIPS

Many businesses that have been operating under the impression that they had until the end of 2019 to bring themselves into compliance with California's new sweeping privacy law will now need to speed up their privacy compliance efforts in order to ensure compliance with Nevada's new opt-out requirement by October 1, 2019. Given the extremely limited window of time before Nevada's new opt-out requirement takes effect, covered businesses should take immediate steps now to make the necessary changes to bring themselves into compliance by the law's effective date.

A good starting point for compliance is for companies to ensure that they are continuing to maintain compliance with the requirements of Nevada's original consumer privacy law, which mandates that covered entities post a notice that identifies and describes:

- the categories of covered information collected by the company;
- the categories of third parties with whom the company shares covered information;
- the company's process for consumers to review and request changes to their covered information;
- the company's process for informing consumers of material changes to its notice; and
- an indication whether the company collects covered information pertaining to individual consumers' online activities.

While SB-220 does not impose an express obligation to provide notice to consumers of their right to opt out of the sale of their personal data, businesses should update their public-facing privacy notices to include a description of how consumers can lodge opt-out requests. Given how narrowly a "sale" is defined, not all operators engage in sales of covered information under the Nevada law. If you are an operator and you do not sell covered information, you may wish to simply state this in your privacy notice. Operators will need to determine how to help users distinguish between a "sale" for purposes of exercising their rights under California law and a "sale" for purposes of exercising their rights under Nevada law.

Second, covered businesses must establish a designated request address for consumers to submit opt-out requests. Fortunately, covered entities have some flexibility in complying with this requirement, and can utilize a dedicated e-mail address, toll-free telephone number, or website for users to submit opt-out requests.

Third, covered businesses must establish systems and procedures for receiving opt-out requests, as well as a process for reviewing and verifying consumers' requests. SB-220 does not provide any guidance on how covered entities should verify the validity and authenticity of a consumer's request. Instead, the new law only provides that a covered entity must "reasonably verify the authenticity of the request and the identity of the consumer *using commercially reasonable means*." One effective method for verification is with the use of the consumer's account that is maintained with the company, whereby verification can be completed through the consumer's login credentials. Alternatively, covered entities can also utilize industry recognized standards, such as the National Institute of Standards and Technology's ("NIST") digital identity guidelines, to serve as a template for fashioning organizational verification protocols.

Fourth, covered businesses must ensure that they have the proper policies and practices in place to facilitate the fulfillment of consumer opt-out requests within the 60-day time period that is mandated by SB-220. Here, companies should develop, implement, and document a clear, easy-to-understand opt-out compliance procedure that streamlines the process for handling and satisfying opt-out requests to ensure that no covered data of any consumer who has opted out is sold following the receipt of an opt-out directive.

Finally, covered businesses should train their employees on how to properly handle opt-out requests from consumers. In particular, companies should consider incorporating a specific Nevada opt-out module into their general privacy training regimen, and role-specific training for those employees who will be directly involved in handling opt-out requests from consumers.

For additional information, please contact:

Jennifer J. Daniels
412.932.2754 | Daniels@blankrome.com

David J. Oberly
513.362.8711 | doberly@blankrome.com