



## Privacy & Cybersecurity Update

October 2019

### Nevada's "Opt-Out" Privacy Law and the Future of Data Protection

October 1, 2019 marks a major milestone for data privacy within the United States as Nevada's novel data privacy law comes into force. Nevada joins California in providing consumers with substantial new privacy rights, marking a significant expansion of the state data privacy landscape and signaling new frontiers in the patchwork of state data protection laws.

The law grants consumers data privacy rights related to how businesses can collect, use and sell their personal data. The law not only impacts organizations conducting certain types of business in Nevada, but is also a precursor to similar provisions set forth in the California Consumer Privacy Act, as amended (CCPA) and other data protection bills being drafted and debated across U.S. state legislatures. In addition, failing to comply with the law can be costly, as Nevada's attorney general is empowered to impose civil penalties up to \$5,000 per violation to businesses that, either directly or indirectly, violate the law.

#### The Scope of Nevada's Data Privacy Law

Nevada's new data privacy law applies to "operators" that (i) own or operate a website or provide online services for commercial purposes, (ii) collect and maintain certain types of personal data on consumers who are Nevada residents and access the website or services, and (iii) otherwise engage in activities within the state. For purposes of Nevada's law, personal data (or what the law refers to as "covered information") is defined as any one or more of the following items of personally identifiable information:

- A first and last name

- A home or other physical address
- An e-mail address
- A telephone number
- A Social Security number
- An identifier that allows a specific person to be contacted either physically or online
- Any other information concerning a person collected from the person through the Internet 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

Unlike other data privacy laws, like the CCPA, Nevada's law defines "consumer" in the more traditional sense to mean "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."

Finally, the law excludes a third party that operates, hosts or manages a website or online service on behalf of its owner or processes information on behalf of the owner of a website or online service. It also excludes financial institutions subject to the Gramm-Leach-Bliley Act and entities subject to the Health Insurance Portability and Accountability Act of 1996. It also does not apply to motor vehicle manufacturers or repair services that collect, generate and retain a consumer's personal data, at least to the extent such personal data is retrieved from a motor vehicle in connection with a technology or service related to

the motor vehicle, or provided by a consumer in connection with a subscription or registration for a technology or service related to the motor vehicle.

### **Nevada's "Opt-Out" Right for Consumers**

Nevada's new data privacy law affords Nevada consumers the right to direct an operator (as defined above) to refrain from the sale of any of his or her personal data that the operator has collected or will collect about the consumer. In turn, the law also places a burden on operators to establish a designated request address (e.g., e-mail address, toll-free telephone number, website process) to enable consumers to submit such requests related to the sale of their information, and respond to verified "do not sell" requests submitted by a consumer within 60 days after receipt, although the timeframe may be extended by an additional 30 days if an exception applies.

For purposes of the Nevada law, the term "sale" means the exchange of such personal data "for monetary consideration by the operator to a person for the person to license or sell" the data to additional persons. However, the term does not include the disclosure of personal data by an operator to a third party (i) that processes the data on its behalf; (ii) with whom the consumer has a direct relationship for the purposes of providing a product or service requested by the consumer; or (iii) for purposes which are consistent with the reasonable expectations of a consumer considering the context in which the personal data was provided. The term "sale" also does not apply to the disclosure of personal data to a person who is the operator's affiliate, or as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the person assumes control of all or part of the assets of the operator.

### **Preparing for Compliance**

There are several measures that organizations need to undertake in order to comply with Nevada's "opt-out" data privacy law and similar data protection regulations. For example, in order to understand whether they are subject to any data privacy law, businesses need to understand the

types of personal data they collect, from whom, and how they use, retain and transfer it to third parties.

In addition, businesses often have to provide notice of their data processing activities and the rights afforded to individuals from whom they collect personal data. For example, under Nevada's existing data privacy framework, operators are required to post website privacy policies that, among other issues, (i) identifies the categories of personal data that the operator collects through its website or online service, (ii) identifies the categories of third parties with whom the operator may share such data; (iii) provides a description of the process (to the extent it exists) for consumers to request changes to their personal data; (iv) describes the process by which the operator will make material changes to the notice; and (v) discloses whether a third party may collect personal data about an individual consumer's online activities over time and across different websites or online services when the consumer uses the website or online service of the operator. Businesses should now consider whether they need to include in their website privacy policy, or through other mechanisms (such as "do not sell" links), a description of how consumers can exercise their right to submit "do not sell" requests.

Finally, organizations need to establish mechanisms for receiving verifiable requests and have internal processes to respond to such requests in the limited timeframe permitted under the law. Unlike the CCPA, Nevada's law provides businesses some degree of flexibility regarding how they can receive "do not sell" requests, and businesses should seek, where possible, to leverage existing tools or processes to do so. Moreover, businesses need to have a mechanism for not only altering their business processes to limit the "sale" of consumers' data when requested, but to also implement procedures for notifying the consumer of the same and ensuring such limitations are not inadvertently altered without the consent of the consumer.

**FOR MORE INFORMATION**

For more information, please contact:

**Thomas F. Zych**

216.566.5605

[Tom.Zych@ThompsonHine.com](mailto:Tom.Zych@ThompsonHine.com)

**Steven G. Stransky**

216.566.5646

[Steve.Stransky@ThompsonHine.com](mailto:Steve.Stransky@ThompsonHine.com)

**Mona Adabi**

202.263.4147

[Mona.Adabi@ThompsonHine.com](mailto:Mona.Adabi@ThompsonHine.com)

*This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgment of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.*

*This document may be considered attorney advertising in some jurisdictions.*

© 2019 THOMPSON HINE LLP. ALL RIGHTS RESERVED.