DATA PRIVACY AND CYBERSECURITY

NEVADA'S NEW PRIVACY BILL REQUIRES WEBSITE OPERATORS THAT COLLECT INFORMATION ABOUT CONSUMERS TO UPDATE PRIVACY POLICIES BY OCTOBER 1, 2019

by Sara H. Jodka

While most U.S. companies have been focused on complying with the California Consumer Protection Act (CCPA), which goes into effect January 1, 2020, Nevada quietly passed its own privacy law, Senate Privacy Bill No. 220 which **goes into effect October 1, 2019**. While Nevada's new law is significantly watered down from the CCPA, the law does have a number of external- and internal-facing compliance requirement that those falling within its enforcement crosshairs will need to comply, and fairly quickly.

Entities that must comply are Operators *i.e.*, companies that operate a website or online service that collects Personal Information of Nevada Consumers. This means that even companies that do not have physical operations in Nevada will be subject to the law if they have an online platform of any kind that targets and collects Personal Information of Nevada Consumers.

Specifically, the law requires an Operator to provide Nevada Consumers notice of a designated address they can use to submit a verified request directing the company not to sell any of the Consumer's Personal Information. It also requires Operators to respond to these requests, as detailed more fully below.

But first, as you can tell, there are a number of defined terms that require further clarification.

The Definitions

First, the law only applies to Operators, which means a person or company who/that:

1. owns or operates an Internet website or online service for commercial purposes;

2. collects and maintains Personal 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, or purposefully avails itself of the privilege of conducting activities in Nevada, or otherwise engages in any activity that constitutes enough nexus with Nevada to satisfy the requirements of the United States Constitution.

A "Consumer" covered by the law is 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.

"Personal Information" means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:

1. Social security number.

2. Driver's license number, driver authorization card number or identification card number.

3. Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.

4. A medical identification number or a health insurance identification number.

5. A username, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.

"Designated Request Address" means an electronic mail address, toll-free telephone number or Internet website established by the Operator that a Consumer can submit a verified request to the Operator not to sell the Consumer's Personal Information.

The terms "sale"/"sell" is far more narrow than the same terms used in the CCPA and mean the exchange of covered information, *i.e.*, Personal Information for monetary consideration by the company to a person for the person to license or sell the covered information to additional persons.

Exclusions

The law does not apply to:

1. an entity that is regulated by the Gramm-Leach-Bliley Act (GLBA) or the Health Insurance Portability and Accountability Act (HIPAA) so financial institutions and healthcare providers are not included; or

2. a service provider to an operator; or a manufacturer of a motor vehicle or a person who services a motor vehicle who processes covered information that is either (1) retrieved from a motor

vehicle in connection with a technology or service related to the motor vehicle, or (2) provided by a consumer in connection with a subscription or registration for a technology or service related to the motor vehicle.

Process for Responding to a Request

In response to a request via a Designated Request Address, the Operator must verify the identity of the requestor to ensure they are properly responding to the correct person with the correct information. The Operator must verify the request fairly quickly because it must provide a response to the request within 60 days from the receipt of the request, not from its internal verification of the requestor's identity. The Operator may extend the 60 days to an additional 90 if it decides it is reasonably necessary. The Operator will have to document the reasons supporting the "reasonably necessary" extension, which can be inability to verify the requestor's identity if the facts line up.

Next Steps

Persons or companies that operate websites that collect Personal Information from Nevada Consumers, *i.e.*, Operators will need to post a Designated Request Address, *e.g.*, email, toll-free telephone number or Internet website and inform Consumers how they submit requests not to have their Personal information sold.

The outward-facing work is fairly easy to comply with since the easiest thing to do is to add a section to the company's current website privacy notice with the compliant language. It is even easier given that under current Nevada law, website operators are already required to post a privacy notice that does the following:

- identifies the categories of information the operator collects through its website/online service about users and the categories of third parties with whom the operator may share the information;
- provides a description of the process, if any, for a user to review and request changes to their collected information;
- describes the way the operator will notify users of material changes to the website or online service notice;
- discloses whether a third party may collect information about a user's online activities over time and across different websites or online services; and
- states the effective date of the notice.

Internally, covered entities will need to establish a verification process for handling Consumer requests and procedures for proper documentation. The process will need to include tracking the date of request receipt, status, and completion date; responding to the Consumer regarding eligibility, availability of the legal protection, and application; and updating internal databases that the Consumer's Personal Information may not be sold. Thus, the internal-compliance piece of the new law is more daunting, but privacy counsel can assist with solutions.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of Data Privacy and Cybersecurity law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Sara H. Jodka, CIPP-US is a Member in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.