Bureau Veritas Bulletin

California and Nevada Regulations to Address Security and Privacy of Connected Devices

The California Consumer Privacy Act (CCPA) has been signed into law, resulting in requirements for businesses to provide reasonable security measures when handling personal information, taking steps to protect this information, and dispose of it when it is no longer necessary. This act amends Part 4 of Division 3 of the California Civil Code.

This act requires manufacturers to equip products with security features appropriate to the nature and function of the device in question, and to any information collected, contained, or transmitted, and must provide a design to protect against unauthorized access, modification, destruction or disclosure of information.

Nevada has also passed SB220, which prohibits operators of websites or online services from selling certain information if directed by the consumer to not sell it. The consumer information covered by this regulation includes name, physical address, email address, telephone number, and social security number.

Under this law, operators must provide a designated request address for consumers to request the sale of their personal information be prohibited.

Background Information:
The intent of the California law is to inform consumers with knowledge of personal data being collected and how this data is handled, as well as to provide consumers with access to their own personal data, and an option to prevent the sale of personal data.

Additionally, product service and pricing shall not be impacted by exercising privacy options.

Smart product manufacturers will be required to provide protection for sensitive data, and to properly delete any such data when no longer necessary for the intended function of the device.

Covered devices include those that can connect to the internet, even indirectly, and those that can connect to other devices.

The Nevada law is intended to offer the consumer the right to request that personal information not be subject to third party data sales.

New Requirements:
The new California requirements go into effect on January 1, 2020. All smart devices will need to comply with the new data security requirements at that point.

Internet of Things (IoT) devices must be equipped with reasonable security measures that are:

- appropriate for the nature and function of the device
- appropriate for the information handled by the device
- designed to protect the device and any collected information from access by any party not authorized by the consumer

The Nevada law will take effect on October 1, 2019.

A number of other states are considering similar legislation. Hawaii, Maryland, Massachusetts, New Jersey, New Mexico, Rhode Island, and Washington have proposed laws to address data security. These proposals are largely in alignment with the CCPA.

Bureau Veritas offers evaluation of these characteristics, employing principles from the NIST Privacy Framework to determine compliance.

Additional information:
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
https://www.nist.gov/sites/default/files/documents/2019/04/30/nist-privacy-framework-discussion-draft.pdf

How Does this Impact You? Contact Us to Discuss
If you have any comments and/or questions, please contact your customer service representative or email us at info@us.bureauveritas.com