WINSTON & STRAWN LLP

BLOG

Oregon Becomes Second State to Pass Internet of Things Data Security Law

AUGUST 21, 2019

In May, Oregon became the second state to pass a law with security mandates for Internet of Things ("IoT") devices. Like its California predecessor, House Bill 2395 will take effect on January 1, 2020, and requires manufacturers of Internet-connected devices that are sold or offered for sale in Oregon to equip the devices with "reasonable security features" designed to protect against unauthorized access, destruction, use, modification, or disclosure.

The law only applies to "manufacturers" and defines a "connected device" as any device or other physical object that is capable of connecting to the Internet directly or indirectly, is assigned an IP or Bluetooth address, "and is used primarily for personal, family, or household purposes." The latter requirement is unique to the Oregon bill and seemingly narrows its scope. But the bill is silent as to what constitutes "personal purposes," so manufacturers should be mindful that this definition could be broadly construed. Another unique feature to the bill is that a violation will be considered "an unlawful trade practice" under Oregon's consumer protection law (ORS 646.607). "….A violation of HB 2395 constitutes a violation of Oregon's consumer protection law. A violation of the Oregon consumer protection law may result in an enforcement action by the Oregon regulator, with penalties including investigative actions, injunctive mandates and, for willful violations, fines of up to $25,000 per violation."

While the law is intentionally vague as to what constitutes a "reasonable security feature," it provides some broad parameters and examples of specific approaches that may satisfy the requirement. This includes (1) a preprogrammed password that is unique for each device; or (2) a requirement that a user generate a new means of authentication before gaining access to the connected device for the first time. Lawmakers and regulators have compiled guidance documents—such as guidelines from the Federal Trade Commission and National Institute of Standards and Technology—that outline best practices and security features that may qualify as "reasonable."

The bill reflects the nation's growing awareness of the importance of privacy and security regulations. Indeed, Illinois, Massachusetts, Maryland, New York, and Vermont have all introduced similar bills to regulate the security of connected devices, and members of Congress have introduced the Internet of Things Cybersecurity Improvement Act (S.734). While these bills have either stalled or not yet passed, IoT device manufacturers should monitor ongoing developments in the law.

TIP: Manufacturers will be best positioned to comply with the emerging privacy and data security laws by implementing data security by design to assess legal obligations during the design of products.

2 Min Read

Related Locations

Houston | Los Angeles

Related Topics

Internet of Things (IoT)

Related Capabilities

Privacy & Data Security | Technology, Media & Telecommunications

Related Regions

North America

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.