WINSTON & STRAWN LLP

BLOG

California Passes First State Law Requiring Manufacturers to Secure Internet-Connected Devices

NOVEMBER 5, 2018

Last month, California became the first state to pass cybersecurity- and IoT-related legislation (Title 1.81.26 "Security of Connected Devices") mandating manufacturers of Internet-connected devices to equip their products with security features to prevent unauthorized access and unauthorized use or disclosure of information contained therein. *See* Cal. Civ. Code §1798.91.04(a)(3).

Aimed at protecting in-state consumers against privacy and security breaches posed by the multitude of unregulated smart devices that increasingly permeate and monitor our everyday lives, Cal. Civ. Code §§1798.91.04 – 1798.91.06 requires manufacturers to equip applicable devices with "a ***reasonable*** security feature or features" that are "[a]ppropriate to the nature and function of the device" and "to the information it may collect, contain, or transmit." Cal. Civ. Code §1798.91.04(a)(1) & (a)(2). Among other things, if a device permits user authentication outside of a LAN, the new law requires the manufacturer to either supply unique passwords for the device or force users to change the password before being able to use it. *See* Cal. Civ. Code §1798.91.04(b).

With narrow exceptions, this new law applies to any hardware manufacturer (or agent thereof) who makes a device for sale in or to California that is capable of directly or indirectly connecting to the Internet and that is assigned an Internet Protocol (IP) or Bluetooth address. It does not appear to apply to devices that were not originally intended for sale in California and merely resold there, and does not impose similar burdens on mere software providers or app stores. *See* Cal. Civ. Code §1798.91.06(b). The regulation will be in effect starting January 1, 2020, and enforced exclusively by the Attorney General or city, county, or district attorney. *See* Cal. Civ. Code §1798.91.06(e) & (i).

TIP: Because this new law does not define "reasonable security features" (except in the context of authentication), manufacturers of smart consumer electronics and personal network devices targeting the California market should, at a minimum, incorporate security protocols appropriate to the devices' role in the household and the sensitivity of the personal data collected, and monitor interpretations of the new law as it is applied.

1 Min Read

Author

Gino Cheng

Related Locations

Los Angeles

Related Topics

Data Breach

Consumer Privacy

Related Capabilities

Privacy & Data Security

Related Regions

North America

Related Professionals

Gino Cheng

Steven Grimes

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.