SQUIRE PATTON BOGGS

California Passes First Cybersecurity Law Regulating IoT Devices

California has become the first state in the US to adopt a cybersecurity law governing Internet of Things (IoT) devices.

Senate Bill No. 327, signed September 28 by California Governor Jerry Brown, will go into effect January 1, 2020. While the law might be a great first step in the right direction to regulate a rapidly growing industry and improve the security of IoT, it is short on details as to the type of security features that are expected.

The law will require manufacturers of connected devices (defined as "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address") to equip such devices with a "reasonable" security feature(s) that is appropriate to the nature and function of such device and the information that it may collect, contain or transmit. The security feature(s) must protect the device and any personal information it contains from unauthorized access, destruction, use, modification or disclosure. The law will apply to manufacturers of connected devices sold or offered for sale in California.

If a connected device can be accessed outside a local area network with a password, the device must either:

- Come with a password unique to each device, or
- Require consumers to set a password (other than the default) before accessing the device for the first time.

Other than these specific authentication requirements, the law does not specify what constitutes "reasonable security features."

Limits of the Law

- The law will not impose a duty on manufacturers of connected devices related to unaffiliated third-party software or applications that the consumer voluntarily adds to a connected device.
- The law will not apply to connected devices that are subject to security requirements under federal law, regulations or a federal agency pursuant to its regulatory authority, such as products currently regulated by the FDA.
- The law does not provide a private right of action for consumers.
- The law does not impose a duty on electronic stores or marketplaces to monitor or enforce compliance with the law by the IoT device manufacturer.
- The law does not impose a duty on manufacturers to prevent end-users from modifying the software running on the IoT device.

What May Lie Ahead

The California law may spur further legislation. Currently, a number of measures are on the table at the federal level, including the Internet of Things Cybersecurity Improvement Act, Securing IoT Act, Cyber Shield Act, SMART IoT Act and DIGIT Act. We will be following developments in this area and providing updates, as appropriate.

If you have any questions or concerns regarding SB 327, how it may apply and impact your business, and what steps you should take to comply with its provisions prior to January 1, 2020, please contact one of the lawyers listed.

Contacts

Robin B. Campbell
Partner, Washington DC
T +1 202 457 6409
E robin.campbell@squirepb.com

Elliot R. Golding
Partner, Washington DC
T +1 202 457 6407
E elliot.golding@squirepb.com

India K. Scarver
Associate, Columbus
T +1 614 365 2719
E india.scarver@squirepb.com