Crowell

CLIENT ALERT

Oregon Latest State to Require Reasonable Security for IoT Devices

June 7, 2019

On May 30, 2019, Oregon became the most recent state to mandate basic security on internet-connected devices with Governor Kate Brown's signature on H.B. 2395. Oregon's new statute follows the model of several other states that have introduced or enacted laws requiring security for internet-connected devices. Similar to a California law passed in September 2018, Oregon's law requires manufacturers of "connected devices" to equip such devices with "reasonable security features." California and Oregon's laws will both go into force on January 1, 2020.

Oregon's law largely tracks California's 2018 statute, though one key difference appears in its definition of "connected device." Oregon limits the definition of "connected device" to "any device or physical object that connects directly or indirectly to the Internet *and is used primarily for personal, family or household purposes*." In contrast, California's law applies more broadly to "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol or Bluetooth address."

Also notable is where Oregon followed California's lead. Both laws describe "reasonable security features" as methods to protect a connected device that are "appropriate to the nature and function of the device" and the "information it may collect, contain or transmit" – despite criticisms that the definition is fraught with equal parts flexibility and uncertainty. Both also explicitly identify the following mechanisms for authentication from outside a local area network as "reasonable security features":

A. A preprogrammed password that is unique for each connected device; or
B. A requirement that a user generate a new means of authentication before gaining access to the connected device for the first time.

Like California, Oregon generally carves out any security requirements imposed on connected devices by federal law or regulation, and separately explicitly exempt entities or persons that are subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Other state legislatures currently considering similar security requirements for connected devices include Illinois (H.B. 3391), Maryland (S. 553/H.B. 1276), and New York (S.3975/A.B. 2229).

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Cheryl A. Falvey
Partner – Washington, D.C.
Phone: +1.202.624.2675
Email: cfalvey@crowell.com

Kate M. Growley, CIPP/G, CIPP/US

Partner – Washington, D.C.
Phone: +1.202.624.2698
Email: kgrowley@crowell.com