Oregon became the latest state to require manufacturers of internet “connected devices” that make, sell or offer to sell the devices in the state to equip the device with “reasonable security features” according to Oregon House Bill 2395 amending ORS 646.607.

According to the law, “[R]easonable security features” means methods to protect a connected device – and any information the connected device stores – from unauthorized access, destruction, use, modification or disclosure that are appropriate for the nature and function of the connected device and for the type of information the connected device may collect, store or transmit.

The law goes on to define a “reasonable security feature” as:

- (a) A means for authentication from outside a local area network, including:
  - (1) a preprogrammed password that is unique for each connected 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; or
• (b) Compliance with requirements of federal law or federal regulations that apply to security measures for connected devices.

Oregon’s law is similar to one in California in that it uses the same “reasonable security features” language, which we wrote about a few months ago, CA Civ. Code § 1798.91.04 (2018). Both of these laws take effect on January 1, 2020.

Why is this important? A preprogrammed unique password, or the requirement that a new user of the device generate a new means of authentication prior to using the device for the first time, ensures that your new smart device won’t have the same default password as everyone else’s device. These features also provide additional security so that your IoT device will be less susceptible to spying or hacking. Given the estimate of the number of IoT devices around the world to be in the billions, and that people value the convenience of the devices but don’t want to sacrifice privacy, it’s more important than ever that IoT devices have at least “reasonable security features.”