Expert Analysis

What New Calif. Law Means For Connected Medical Devices

By **Michael Buchanan and Michelle Bufano**
October 5, 2018, 2:09 PM EDT

Michael Buchanan

Michelle Bufano

On Sept. 28, California governor Jerry Brown signed into law SB 327, the first-ever state legislation aimed at regulating internet of things devices. This new law comes just months after California made waves by passing a consumer data privacy law that's been called the nation's toughest, stopping companies from selling personal information without permission from customers.

The new law requires the manufacturer of an internet-connected or "smart" device to ensure that it has "reasonable" security features to "protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure." Products subject to this new law might include smart watches, smart thermostat controls, security systems and even devices like Amazon Echo and its competitors.

While the law does not explicitly define a "reasonable security feature," it must be suitable for the nature and function of both the device and type of information collected. The law applies to products sold or offered for sale in the state of California. The law — which goes into effect on Jan. 1, 2020 — does not create a private right of action, but vests government lawyers with enforcement authority.

The law specifically does not apply to "any connected device the functionality of which is subject to security requirements under federal law, regulations, or guidance promulgated by a federal agency pursuant to its regulatory enforcement authority." Thus, California regulators are not authorized to bring an enforcement action against a medical device manufacturer governed by any nonbinding U.S. Food and Drug Administration guidance or

other federal regulations.

This first-of-its-kind law addresses the appropriate means of device authentication where a device is capable of connecting to wide-area networks, including public networks. For those devices, the new law requires that the device have a unique preprogrammed password, or that the user generate a new means of authentication prior to initial access to the device. This means that generic default credentials for a hacker to guess will no longer cut it.

Although groundbreaking in its entirety, two of the most interesting aspects of the new law are: (1) a liability carve-out for manufacturers in the event a user alters the software or firmware running on a connected device; and (2) a restrictive definition for a "connected device."

This manufacturer liability exemption will likely set the tone for private causes of action brought under negligence or strict product liability theories. Under traditional tort law, a manufacturer's liability for a defect is limited to a tangible product. But manufacturer liability for personal injury resulting from interconnected devices is new ground, where both the tangible device and less tangible technology combine to produce device functionality. Thus, the scope of a manufacturer's duty in this realm remains unclear, and the new law's recognition that a manufacturer is not liable to the government where the user has modified the software may provide useful guidance in the civil context.

A manufacturer can be held liable in the traditional tort context for reasonably foreseeable misuse of a product by the user, including reasonable modifications made by the user to the product. This is true for interconnected medical devices falling within the scope of the FDA's nonbinding guidance relating to interoperable medical devices issued in September 2017. The FDA has seemingly adopted the tort concept of foreseeable misuse in the cases of "reasonably foreseeable misuse, and reasonably foreseeable combinations of events that could result in a hazardous situation."

The new California law, on the other hand, exempts a reasonably foreseeable consumer alteration as a source of liability. The state legislature's recognition that a manufacturer is not liable under these circumstances should provide some guidance in determining and limiting a manufacturer's liability when these sorts of claims arise.

Additionally, the new law also may influence the extent of civil liability for a product defect

vis-à-vis its restrictive definition of a connected device. The scope of what is considered the “product” or device is critical in a strict product liability context, because only the product manufacturer can be held liable for a product defect.

Here, the new statute defines a “connected device” 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.” Thus, the use of the phrase “physical object” in the definition of the devices subject to the new law, at least arguably, appears to limit liability to only the manufacturer of a tangible device, and does not extend liability to other entities, such as software developers, that contribute to the functionality of the device.

This definition differs in scope from the FDA guidance specific to internet-connected medical devices, issued in 2015. That FDA guidance defines medical devices in a way that is not limited to the tangible device, as the new California law appears to. Instead, the FDA guidance states that products “that are built with or consist of computer and/or software components or applications are subject to regulation as devices when they meet the definition of a device in section 201(h) of the FDIC Act.”

Section 201(h) defines a device as “an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory” that is “intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man” or “intended to affect the structure or any function of the body of man or other animals. ...” Thus, pursuant to the FDA guidance, software or applications — not just tangible hardware — may be considered a part of the “device” if “intended for use in the diagnosis or the cure, mitigation, treatment, or prevention of disease, or to affect the structure or any function of the body of man.”

In a strict liability/design defect situation, no court has yet defined “device” in the context of interoperable medical devices, which derive their functionality from technology such as apps. How "device" is defined is critical to determining liability — i.e., is only the manufacturer of the physical device liable, or does liability also extend to those involved in the technology that makes the device functional? The new California law draws a narrower line as to potential liability than the FDA guidance. Only time will tell how courts will ultimately parse liability in this context.

Michael F. Buchanan and Michelle M. Bufano are partners at Patterson Belknap Webb & Tyler LLP.