Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Calif. Starts Ball Rolling With Novel Internet Of Things Law

By **Allison Grande**

Law360 (September 17, 2018, 8:58 PM EDT) -- California is poised to become the first state to enact rules mandating security features for internet-connected devices, marking a modest first step in what is likely to be a flurry of activity in the coming years to more tightly regulate emerging technologies at the state and federal levels, experts say.

Makers of televisions, routers, fitness trackers, automobiles, refrigerators and a range of other devices that connect to the internet as part of the rapidly growing "internet of things" would be required under Senate Bill 327 to equip products with "reasonable security features." That includes ensuring that passwords are not as easy to hack. California lawmakers passed the bill late last month and the measure awaits the signature of Gov. Jerry Brown, who must act before Sept. 30.

The legislation is notable for both its narrowness and flexibility, according to experts, who viewed the first-of-its-kind bill as a precursor to, and potential model for, a nationwide standard for protecting personal data in an increasingly connected world.

"This action is a first but very small step in what I anticipate is going to be an emerging area of the law over the next five to 10 years," said Ballard Spahr LLP partner David Stauss. "The number of internet of things devices is expected to expand exponentially with the growth of technologies such as smart cities and autonomous vehicles, so there's a big push for states and the federal government to figure out how to control these devices."

Determining how to effectively regulate an emerging industry that has yet to face formal privacy or security mandates is likely to present a challenge, experts acknowledged, although the narrowly tailored approach of the California privacy law could provide some valuable insights.

The California bill was drafted in response to a string of high-profile incidents where connected devices such as routers and baby monitors with easy-to-guess default passwords have been hacked.

The most notable of these breaches came in October 2016, when attackers hijacked internet-connected devices around the globe to flood domain service provider Dyn with malicious traffic, resulting in access to Twitter and other popular websites across the internet being temporarily blocked.

The California legislation, which would take effect in January 2020 if enacted, requires companies to institute "reasonable" security features or features that are "appropriate" to guard against intrusions given the nature, function and data collection capabilities of the connected device. The bill defines

connected devices broadly 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."

The Federal Trade Commission mandates that businesses adhere to “reasonable security” measures, but the open-ended definition of “reasonable” has come under fire by companies that make connected devices. The California law, by contrast, imposes a clear burden on companies to protect their devices with unique passwords or force users to set their own password during its first use.

"The legislation raises the question of what is reasonable security, but then gives the answer in the next clause," Stauss said. "By stating that manufacturers need to force a password change or send out devices with unique passwords, that gives manufacturers a path to compliance."

The bill is enforceable only by California's attorney general or a city attorney, a county counsel or a district attorney and does not contain a private right of action. But some attorneys expect the plaintiffs' bar, which is expected to ramp up its activity in this space in the near future, to seize on the new security requirements if there's a breach or other major security incident involving a device that allegedly lacked proper password security.

"If you're an IoT manufacturer and can put your hand up and say, ‘I've complied with this law and now force password changes,’ that should help in litigation [by] being able to argue that ‘the law says to do “X,” and I did it, so I'm not negligent,’" Stauss said.

But while the additional detail about what constitutes "reasonable security" is illuminating, it's not overly rigid, leaving businesses that manufacture or contract to manufacture connected devices sold or offered for sale in the Golden State with room to adapt to a rapidly evolving environment, experts say.

"The 'reasonable security' standard is quite flexible, which is good when operating in a world where both the devices and threats are constantly changing," said Covington & Burling LLP partner Lindsey Tonsager. "As with the standards put forth by the FTC, the California legislation recognizes that reasonableness is not going to be the same for every company and it's going to depend on different factors, including the type of the information collected and the functionality of the device."

The balance between specificity and flexibility struck by the California bill is likely to appeal to many in the connected device industry, who may come to view the legislation as a de facto national standard due to the impracticability of building devices with compliant password settings just for California, experts say.

"The challenge is that there is such a broad diversity of devices that constitutes the internet of things right now that it's really hard to make across-the-board rules," said Tommy Ross, senior director of policy at BSA: The Software Alliance. "By not requiring manufacturers to use default or hardcoded passwords in general, but rather requiring that default passwords not be used only in cases where manufactures have already chosen to use passwords, that's a good example of a little more nuanced approach that is helpful in this space."

However, while the California legislation — which does not apply to manufacturers that are already regulated by the federal Health Insurance Portability and Accountability Act or California's health privacy law — is likely "to impose some additional rigor" for IoT companies that have yet to be extensively regulated, the net effect of the new rules may be fairly limited, according to Wiley Rein LLP privacy and cybersecurity practice chair Kirk Nahra.

"This law may have some actual impact on pushing security concerns higher on the priority list, but I'm not sure it will really do too much to make sure that companies actually go beyond what they have been doing today or thinking about today," Nahra said.

Marc Rotenberg, the president of the Electronic Privacy Information Center, agreed that while the California legislation is "a step in the right direction because it recognizes the risk of IoT devices, it is also a very modest proposal because it does not recognize that IoT devices can be both the target of the attack and the gateway to the attack target."

"Also, there are safety risks associated with IoT devices that are distinct from privacy issues," Rotenberg added, citing the examples of hackers disabling door locks, changing thermostat settings or remotely activating microwave ovens. "IoT legislation needs to address those risks."

Those issues are likely to factor prominently into the already-initiated push to establish both IoT specific security rules and more general privacy standards to govern emerging technologies in the coming years, experts say.

At the federal level, lawmakers have floated proposals that take a somewhat cautious approach to regulating the emerging connected device space. Both the SMART IoT Act and DIGIT Act call for studies of the industry to be conducted before any formal rules are enacted, and the Cyber Shield Act would set up a voluntary program that would allow businesses to certify that their IoT products meet certain data security standards.

These proposals provide a contrast to how state and federal policymakers are moving to legislate the way companies collect, use and share personal data more broadly.

California has been at the forefront of this movement as well, with the state in June putting on the books a landmark privacy law that gives consumers more control over how companies use and share their personal information online and the ability to request the deletion of this information and to opt out of the sale of their data to third parties.

Federal lawmakers have also demonstrated a growing appetite to put more limits on companies' use of consumer data, with proposals put forth on the heels of the enactment of the European Union's sweeping General Data Protection Regulation in May including requiring data-rich companies to obtain opt-in consent to use, share, or sell personal information and mandating that most public-facing websites and apps craft easily accessible and digestible privacy policies.

"It's interesting that at the same time that we're seeing calls for a federal privacy law and a sweeping new blanket privacy law in California, we're also seeing these really tech-specific measures when it comes to the internet of things," Tonsager said.

Companies are increasingly getting involved in these legislative efforts, particularly at the federal level. Within the past month, the U.S. Chamber of Commerce, BSA: The Software Alliance and the Internet Association — which counts Google, Facebook and Microsoft among its members — have separately put forth privacy principles that they believe should underpin any national privacy legislation.

Shaundra Watson, the director of policy at BSA, told Law360 that the software industry group elected to put together its list of 10 principles after examining the increasingly mature privacy management

programs and best practices being instituted by its members worldwide and finding a common thread when it came to the importance of ensuring consumers have control over what is being done with their data.

"The central theme is that we want companies to be able to still provide important services to consumers, but we also want to make sure they're doing that in a way that allows consumers to be empowered," Watson said.

The privacy principles floated by BSA and other groups could easily apply to a broad range of industries that rely on the collection and use of consumer data, including internet of things manufacturers, Watson said, although she added that the software industry group advocates for a legislative approach that folds the regulation of emerging technologies into a comprehensive framework rather than subjects the industry to its own set of rules.

"These principles absolutely have applications in the internet of things context, but that's not the only context," Watson said. "Technology is evolving at a breakneck pace, so it's really important that solutions be flexible and endurable and that any approach to privacy legislation be uniform and technology neutral."

Ross, the senior director of policy at BSA, noted that the group has long supported building security by design into the development process for the software that fuels internet-connected devices. Given the fledgling nature of the industry, the development and subsequent encouragement of the adoption of a set of minimum best practices for IoT security, rather than inflexible rules, may be the most promising path forward, he said.

"The California bill is a good step to begin the discussion around information security management for IoT devices, but the key to success will be to flush out what reasonable security features mean with a nuanced understanding of the devices that are out there," Ross said.

Attorneys say that with California breaking the ice on both IoT security and online privacy rules in general — as the state has already done with topics such as data breach notification legislation, which came into force in 2003 and has since spread to every other state — it's only a matter of time before other states and the federal government land on ways to regulate what to date has been an industry governed primarily by best practices.

"As these devices become more and more prevalent, and if more manufactures choose not to build security in from the start, lawmakers are more likely to follow California's lead and look to formal rules," Stauss said.

--Editing by Emily Kokoll and Jill Coffey.