California pushed law further into cyberspace on Sept. 28 with the passage of SB-327, the first state law regulating the expanding, amorphous network known as the Internet of Things. And as with most new rules, law firms are in various states of preparedness.

Under SB-327, called the Security of Connected Devices law, thermostats, health monitors, cars and video doorbells connected through sensors to the Internet must be sold with security features. Taking aim at manufacturers, the rule follows stories about thieves accessing databases through hacked fish tanks, military information disclosed by fitness devices and law enforcement raising concerns about toys with Internet connections.

"California said 'This is so screwed up. We have video doorbells, remote locks and they are all vulnerable,'" said John Simek, VP of Sensei Enterprises, a cybersecurity firm catering to law firms in Fairfax, Va. "It's a reaction to breaches of IoT devices and botnets."

The law becomes effective Jan. 1, 2020. On the same day, another California cyberlaw, the Consumer Privacy Act, takes effect. This rule, passed before SB-327, gives citizens more control over personal information collected about them.

The laws are just the latest in a series of rules governing cybersecurity and data protection, and firms are positioning themselves for more. Besides the California laws, a handful of states, including Texas, Illinois and Colorado, have passed data protection laws. The EU's General Data Protection Regulation (GDPR), which became effective this past May, is among the most far-reaching and comprehensive cyberlaws passed.

"This can be a growth area for law firms and privacy experts will be in demand," said Robert McDowell, former commissioner to the Federal Communications Commission and now a lawyer at Cooley LLP. Next up is probably a U.S. federal law, he said. "There's going to be a lot of new law created."

Consumer privacy, data protection, cybersecurity and evidence expertise are among the knowledge areas required for firms to have a well-rounded approach to the new cybersecurity laws. But are they ready? Andrew Grant, a lawyer with Perkins Coie and a partner in its technology transactions and privacy group, said many firms have work to do.

"The level of preparedness is sort of medium level," he said. "IoT isn't a simple area, there are a lot of competing and, sometimes, conflicting issues you have to deal with."

Information technology research firm Gartner predicted last year that 20.4 billion IoT devices, from toasters to toys to oil tanks, will be active by 2020. That's up from 8.4 billion estimated in 2017. Securing those devices will cost $1.5 billion this year, the firm predicted, reaching $2.46 billion in 2020.

According to experts, the five current top cybersecurity and privacy legislations for law practice include:

California's Security of Connected Devices Law: This is the IoT law that goes into effect Jan. 1, 2020. It calls for "a reasonable security feature" on all devices manufactured to connect to the Internet. The legislation raises a variety of issues for law firms, including how evidence is gathered from devices with Internet-connected sensors, and what is allowable and available in discovery.

"Lawyers haven't been as thoughtful as they could about using data from these devices in resolving disputes, in discovery and litigation, in how the devices are going to help," said David Kessler, Head of Data and Information Risk at Norton Rose Fulbright.

California's Consumer Privacy Act :The second California cyberlaw that takes effect Jan. 1, 2020. The rule protects people's right to tell a business not to share or sell personal information, protects people from discrimination if they opt out of sharing or selling private information, and makes businesses responsible for keeping information safe.

This law faces amendments after being rushed through, said Sheryl Falk, co-leader of Winston & Strawn's Global Security and Data Privacy Task Force.

European General Data Protection Regulation (GDPR): The GDPR took effect this past May, after being approved 2 years ago. The law aims to protect EU citizens from privacy and data breaches. It applies to all companies processing the data of people in the EU, no matter where the company is based. Penalties for breaking the law are has high as 4 percent of a company's annual revenue.

California modeled its privacy law on the GDPR, and now U.S. law firms want more information about what the regulation means.

"I was talking at a conference of attorneys general and they wanted to know about GDPR — you could hear a pin drop. The strictest, most comprehensive law is GDPR," Falk said.

Health Insurance Portability Act (HIPAA): HIPAA rules cover health information gathered by so-called implantables, which are IoT connected devices embedded in or worn by a patient. In October the Food and Drug Administration warned that an implantable sold by Medtronic could be exploited by hackers.

"If I have an implantable or wearable that collects health information and my provider can access that info, it could be covered by HIPAA," Kessler said. "Lots of devices in a hospital are Web enabled."

Various State Laws: States have been adding personal information and privacy protections since earlier in the decade and more may be coming. Colorado, Massachusetts, Washington, Illinois and Texas are among states with laws on collecting, storing and disclosing information. Colorado's Protections for Consumer Data Privacy Act became law Sept. 1. Vermont passed a law this year that regulates companies that sell people's information. Massachusetts passed its data protection ruling in 2010.

Washington, Illinois and Texas have all passed laws addressing data collected through biometric devices such as fingerprint readers. "States are increasing their focus on biometric data," Grant said.

Technology has been racing ahead of the rulemakers, and law firms that are able to harness the information, stay abreast of developments while being aware of risks will be the most competitive.

"Our emerging technology has outstripped our regulations," Falk said. "We are all living in a brave new world."