OCTOBER 1, 2020

Legaltech news ONLINE

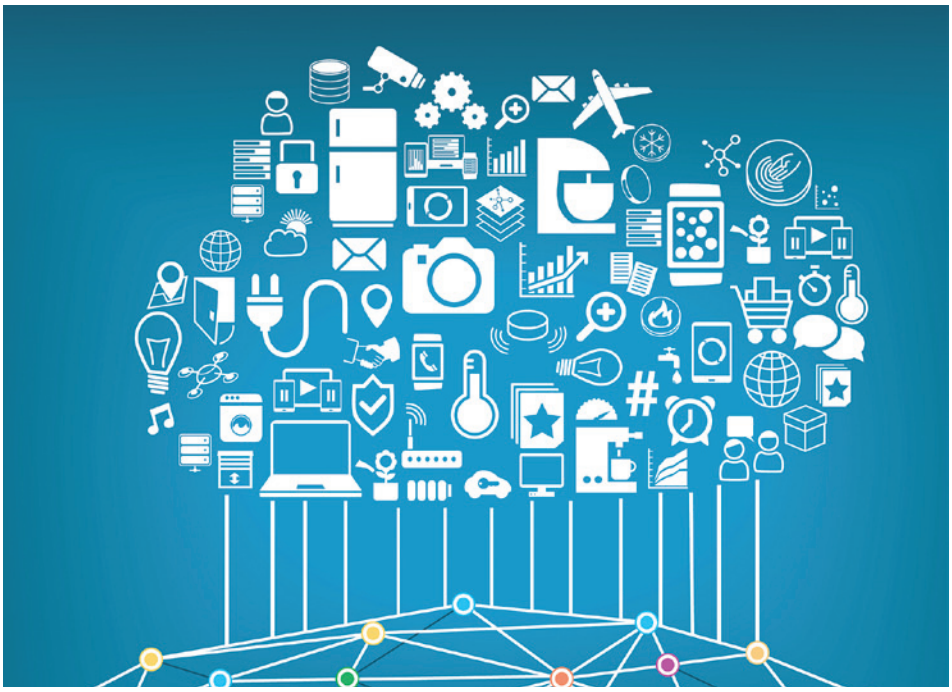
An ALM Publication

FTC Lawyer: Lawmakers 'Working More From A Consensus' Toward IoT Cybersecurity Law

As IoT manufacturers contend with bad actors, U.S. and international regulators are poised to implement more cybersecurity requirements, according to a recent panel at Winston & Strawn's Disruptive Technologies Legal Summit.

BY VICTORIA HUDGINS

Yesterday, a Winston & Strawn panel discussed the emerging U.S. and international laws aiming to regulate the Internet of Things (IoT) market. But stiffer regulations may pose challenges for IoT manufacturers that are still struggling to move security from an afterthought to a critical development element, panelists noted.



The "Focus on Data Security by Design—Protecting Internet of Things (IoT) Devices & Emerging Technology" panel was held virtually during Winston & Strawn and Berkeley Center for Law & Technology's "Disruptive Technologies Legal Summit." Among other topics, the livestreamed event discussed the difficulties with implementing IoT cybersecurity controls.

"One of the challenges is that full development stack," noted Serge Jorgensen, president and founding partner of cybersecurity and digital forensics provider Sylint Group Inc. "Because there's so many components that come together and go into a device that suddenly has internet connectivity, analyzing all those components and understanding the full security of that stack is challenging."

Further complicating security in IoT devices is the fact that security is often an afterthought and not a part of the product development, added Brad Ree, chief technology officer of ioXT, an alliance of manufacturers and government organizations for IoT products.

"What I see too often is the product is about to ship, and

they go to the security team and say, 'Hey, bless this," Ree said. He added, "It's still difficult for them to swallow [and get] the CEO to understand that security and developers should be working together from the get-go so you avoid spending more trying to clean up security."

However, lawmakers appear poised to regulate cybersecurity more closely as IoT products proliferate and hackers find ways to breach them.

Federal Trade Commission assistant regional director of the Southwest region Jim Elliott noted that Senate Republicans introduced the Setting an American Framework to Ensure Data Access, Transparency and Accountability Act (**Safe Data Act**) earlier this month. The legislation would allow Americans to control, access or delete their IoT data, strengthen the FTC to enforce the regulation and implement additional requirements that "would direct businesses to be more transparent and accountable."

However, Elliott noted that Congress' looming session deadline and questions if the Safe Data Act would preempt state law or include a private right of action were "some factors that are working against it." But the proposed legislation signaled progress for implementing a national cybersecurity law, Elliott added.

"Still, we are getting closer and it seems like we're working more from a consensus to provide a much broader framework and more comprehensive program of security," he said.

As the IoT market and their lawyers closely watch the fate of the Safe Data Act, moderator and Winston & Strawn partner Sheryl Falk said there were other regulatory developments to follow concerning IoT devices.

Falk noted the United Kingdom's pending IoT framework, Brazil's IoT plan and a U.S. bill proposing to regulate federal government-purchased IoT devices were noteworthy. There are also regulations already on the books that govern IoT devices that manufacturers should be aware of, she added.

For instance, the General Data Protection Regulation (GDPR) elevated "security by design" from a best practice to a rule, Falk said. The California Consumer Privacy Act (CCPA) also added reasonable security responsibilities onto IoT providers and any other entity that falls under the law's purview.

The FTC likewise regulates IoT devices to ensure they have "reasonable security." Still, Elliott said the FTC acknowledges that data security varies per company and constantly evolves.

"The question we look at is are you ahead of the pack, barely keeping up" or in the middle of the pack, he explained.

To remain compliant, Elliott suggested IoT providers ensure their third-party providers have reasonable security measures, provide patch updates and stay abreast of threats.

Victoria Hudgins

I am a reporter for Legaltech News, where I cover national and international cyber regulations and legal tech innovations and developments.

WINSTON & STRAWN LLP