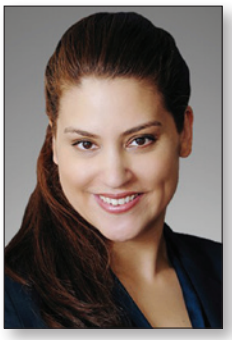
APRIL 6, 2017

Legaltech® news

ONLINE

An ALM Publication

Regulatory Scrutiny Ramping Up in the Rapidly Expanding Internet of Things



Natasha Kohne Crystal Roberts

All three major branches of the federal government, as well as the states, have begun to tackle regulation of the IoT.

BY NATASHA KOHNE AND CRYSTAL ROBERTS, AKIN GUMP

In another effort to regulate privacy and security in the rapidly-expanding internet of things (IoT), the Federal Trade Commission filed a lawsuit earlier this year against D-Link, a global manufacturer of computer networking equipment and other connected devices, for inadequate security practices and deceptive claims regarding the security of its routers, IP cameras and baby monitors. Among other allegations, the FTC alleges—under its authority to regulate unfair and deceptive practices under Section 5 of the FTC Act—that D-Link's security failures allowed unauthorized access to cameras' live feeds and left its routers vulnerable to hacking.

Credit: Vasin Lee/Shutterstock.com

This is one example in a line of cases where a government agency attempts to regulate a relatively new and emerging phenomenon: the IoT. This emerging technology offers great promise and opportunity, but with rapid growth estimated to be 30.7 billion devices by 2020, it is not surprising that we are already seeing all three major branches of the federal government, as well as the states, begin to tackle regulation of the IoT. And as with many technological advancements of this magnitude, both public and private sector action will be necessary to encourage growth while protecting consumer safety.

The FTC's interest in IoT regulation did not start with the D-Link case. The FTC settled its first case in the IoT space in September 2013. There, the FTC alleged that TRENDnet, a marketer of video cameras for home security and baby monitoring, failed to use reasonable security, and its "lax security practices exposed the private lives of hundreds of consumers to public viewing on the internet." In February 2016, the FTC also settled a case against computer

manufacturer ASUSTek Computer for alleged security flaws in its routers. The FTC alleged that the company failed to take reasonable steps to secure the software on its routers, allowing hackers to change routers' security settings without consumers' knowledge and gain complete access to consumers' connected storage devices.

Not all IoT scrutiny from the government has been negative, however. Some senators have served as champions of IoT development to further spur innovation. In early 2015, the Senate Committee on Commerce, Science and Transportation held a hearing on IoT regulation. During the hearing, Sen. Cory Booker, D-N.J., who called for the hearing along with Sens. Kelly Ayotte, R-N.H., Deb Fischer, R-Neb., and Brian Schatz, D-Hawaii, encouraged growth of the IoT over restriction and stated that the government should not "inhibit a leap in humanity."

However, others in the federal legislature have pushed for regulation, including Sen. Richard Blumenthal, D-Conn., and Representatives Frank Pallone, D-N.J, and Jan Schakowsky, D-Ill, on the U.S. House of Representatives' Committee on Energy and Commerce, who pushed for FTC involvement following the well-known DDOS attack that used a botnet of internet-connected devices to attack an internet infrastructure company in October 2016. Highlighting the fact that "IoT devices are the fastest growing category of connected devices," these legislators urged the FTC to "call on IoT device manufacturers to implement security measures" and alert consumers to security risks.

The judiciary has also had to grapple with challenging IoT security questions. In a Northern District of California case against car manufacturers Toyota, Ford and General Motors, the plaintiffs argued in part that the cars' computer systems were vulnerable to hacking, allowing the car to be controlled by individuals outside the car and endangering the safety of drivers and passengers. Limited by the constitutional requirement that plaintiffs must suffer an injury-in-fact, the court determined that a future risk of hacking did not satisfy the standing requirement for purposes of surviving a motion to dismiss. Notably, the case was decided prior to the Supreme Court's decision in Spokeo Inc. v. Robins and is currently on appeal to the Ninth Circuit.

At the state level, state attorneys general have warned against potential privacy and security threats in the IoT. In October 2016, also following the October 2016 DDOS attack, then-California Attorney General Kamala Harris advised Californians "to protect their electronic devices from potential hacks and urge[d] [IoT] manufacturers and developers to take immediate steps to help secure home electronic devices against" potential botnet attacks.

As California has been a leader among the states in enhancing privacy and data security, other states and cities can be expected to shift attention to the IoT. For example, New York City has developed special guidelines to help city agencies understand the risks associated with the IoT and best practices to mitigate these risks.

As with similar advanced technological problems, the public sector is working to find ways to incentivize the private sector to participate in solving privacy and security problems in the IoT. Early this year, the FTC announced a public cash-reward contest, the "IoT Home Inspector Challenge," for tools that "help protect consumers from security vulnerabilities in" the IoT. The FTC is offering up to $25,000 for the best technical solution and $3,000 for honorable mention. The FTC has presented similar challenges in the past, such as the FTC Robocall Challenge in 2012, which incentivized innovative solutions for blocking illegal robocalls on landlines and mobile phones, in return for a $50,000 cash prize. As seen by the FBI's offer of over $1 million to the individual who could hack into the iPhone of a terrorist gunman in San Bernardino, California, private sector talent is essential in producing technological solutions to complex problems.

While regulators, legislatures, the judiciary and the private sector continue to grapple with these cutting-edge IoT issues, we will continue to see developments in resolving IoT security issues at all levels of government and in the private sector. By looking toward regulatory guidance and working with outside counsel, technology companies in particular should take steps to ensure they meet the evolving standards and expectations.

Natasha G. Kohne *is co-leader of Akin Gump's cybersecurity, privacy and data protection practice, assisting clients in the U.S., the Middle East and other international markets. Based in San Francisco, she has also spearheaded Akin Gump's international efforts in relation to data protection and cybersecurity.* ***Crystal Roberts*** *is a member of the firm's litigation and cybersecurity, privacy and data protection practices in San Francisco.*