NEWSLETTER

IoT Security: "I'm From the Government and I'm Here to Help"?

December 2016

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Telecom, Media & Technology

Ronald Reagan joked that the most terrifying words in the English language are: **"I'm From the Government and I'm Here to Help."** When it comes to security and the Internet of Things (IoT), government wants to be helpful, for better or for worse. The National Institute of Standards and Technology (NIST), the National Telecommunications and Information Administration (NTIA), the U.S. Department of Homeland Security (DHS), the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), the National Highway Traffic Safety Administration (NHTSA), and the U.S. Food and Drug Administration (FDA) are all looking at IoT. Congressional IoT interest abounds. As President-elect Trump and a new Congress take over, the fate of ongoing activities is unclear, but widespread interest and divergent approaches at DHS (and other agencies) and on the Hill promise future scrutiny.

On one hand, DHS released a report, *Strategic Principles for Securing the Internet of Things (IoT)*, finding it "imperative that government and industry work together, quickly, to ensure the IoT ecosystem is built on a foundation that is trustworthy and secure." DHS states that the "role of government" is to "provide tools and resources so companies, consumers, and other stakeholders can make informed decisions about IoT security." DHS offers principles to "motivate and frame conversations about positive measures for IoT security among developers, manufacturers, service providers," and consumers. These (unsurprising) principles are:

- Incorporate Security at the Design Phase
- Promote Security Updates and Vulnerability Management (citing NTIA's Multistakeholder Process on Patching and

Updating for IoT)

- Build on Recognized Security Practices (citing the NIST Cybersecurity Framework)
- Prioritize Security Measures According to Potential Impact
- Promote Transparency across IoT (including, among other things, vendor risk assessments and a publicly disclosed way to use vulnerability reports)
- Connect Carefully and Deliberately (targeted at consumers)

DHS offers next steps, including coordination of activities, building awareness of risks, evaluating incentives, and international standards activity. A notable contribution is DHS interest in how "tort liability, cyber insurance, legislation, regulation," voluntary initiatives, and other efforts can improve security. Given recent litigation over aspects of IoT security, the government might help by protecting innovators and companies from class action lawsuits.

On the other hand, some want regulation. Some Democratic Hill staff lament that there are no federal requirements for security in IoT devices. Some commentators think regulation should force manufacturers to meet minimum security standards: Bruce Schneier from Harvard's Berkman Center recently told a House Subcommittee hearing that "the only solution is to regulate. The government could impose minimum security standards on IoT manufacturers, forcing them to make their devices secure even though their customers don't care. They could impose liabilities on manufacturers." Regulation is premature and even agency "guidance" can prejudge technology and stymie innovation.

At bottom, while regulation is exceedingly unlikely in a new Congress and Administration, these sorts of reports provide fodder for agencies struggling with what, if anything, to do about IoT security. More troubling, States may get in on the action, and class action plaintiffs are looking for the next ubiquitous technology that can provide a basis for litigation. Innovators must watch these efforts and look for ways the government can help, not hurt.