wiley

NEWSLETTER

Is 'Managed IoT' the Key to IoT Security?

April 2017

Policymakers considering the Internet of Things (IoT) and security confront a dizzying array of potential devices, services, use cases, and consumers. Commentary jumps from connected fridges to medical devices to industrial sensors, sometimes with scant recognition that end users' expectations are going to differ wildly across settings and evolve over time.

The U.S. Chamber of Commerce's Technology Engagement Center (C_TEC) recently urged the U.S. Department of Commerce to recognize the diversity of IoT, in order to help policymakers avoid oversimplifying IoT or lumping together dissimilar use cases. Those comments are available here.

To be sure, IoT is "things" that are connected, but it is also the connections and the services that support connectivity. Too much focus on devices ignores the complexity of IoT. IoT can be divided up in multiple ways, each of which may be premature as IoT is still evolving. We see consumer IoT and industrial IoT, though those can overlap when commercial devices and services make their way into enterprise settings like retail, hospitality, education, and the workplace. It may be more useful to watch for evolution into what C_TEC described as "managed and non-managed" products and services. We may see dominant platforms emerge, provided by reputable companies, to support consumer use of diverse IoT. We may also see platforms offered to support developers and product manufacturers looking for consistent approaches, interoperability, and more sophisticated life cycle management, including software updates, interaction with networks, and device end of life.

IBM recently offered "Five Indisputable Truths About IoT Security" that underscore the potential importance of managed services to IoT security. These Five Truths address "the importance of partnering with

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Internet of Things
Privacy, Cyber & Data Governance
Telecom, Media & Technology

IoT vendors and solution providers who can be trusted" and the need of "administrators of IoT deployments" to have "visibility and control to deal with" threats and attacks. Indeed, managed services may make it easier to manage life cycle issues and "system defenses," which IBM says "will need to be updated repeatedly – for the life of these devices – impacting the supply chain for both software and equipment."

If the ecosystem evolves toward a managed services approach, it seems unlikely that government intervention or a "nudge" on security would be necessary. Large, experienced companies such as Microsoft, Cisco, Intel, and Amazon Web Services know how to offer large-scale services and support – both off the shelf and customized. They may lead in a similar fashion on IoT development and management, potentially obviating many concerns about security in IoT. The emergence of large-scale managed services could make it easier for policymakers to focus on the most troubling use cases or security risks that remain in the future IoT.

Are managed services a panacea? Probably not, and who knows if the demand for such services will materialize? If it does, will it be at the enterprise level, among consumers seeking to simplify their connected lives, or both? It is too soon to tell. This makes it entirely premature to begin prescribing solutions or have the government put its thumb on the scale. The market will drive development, delivery, and support platforms. Policymakers should look to this rapidly developing ecosystem to see how things unfold. Managed IoT may end up being a welcome solution to many of the technical and operational concerns about IoT security.