Published on *The National Law Review* https://natlawreview.com

Advisory Group Releases Report on Internet of Things

Article By:

David J. Bender

Following ***NIST***'s release of cybersecurity guidance for the *Internet of Things* last week, the ***Broadband Internet Technical Advisory Group (BITAG)*** released a report today titled *Internet of Things (IoT) Security and Privacy Recommendations* (the Report). BITAG is a non-profit organization that brings together engineers and technologists in a working group to develop consensus on technical issues that can affect users' Internet experiences. The Report includes contributions from academics, advocacy organizations, and members of the telecommunications and consumer technology industries, with recommendations designed to "dramatically improve the security and privacy of IoT devices and minimize the costs associated with the collateral damage that would otherwise affect both end users and ISPs."

As used in the Report, IoT refers to "consumer-oriented devices and their associated local and remote software systems." The Report begins with background information about IoT, why IoT security and privacy is of particular interest, and the observation that many IoT devices do not abide by "rudimentary security and privacy best practices." According to the Report, IoT devices therefore pose unique security and privacy challenges because they tend to implicate "non-technical or uninterested consumers" and can widely impact Internet access and other services when the devices are compromised by malware.

The next section of the Report details a series of observations on IoT security and privacy issues. These observations are divided into several categories, including the following:

- *Security Vulnerabilities*: IoT devices ship with software that is outdated or becomes outdated due to the lack of update mechanisms.
- *Insecure Communications*: IoT devices often use unauthenticated and unencrypted communications and also fail to implement authorization and network isolation principles.
- *Data Leaks*: IoT devices may leak user data, both from the cloud and between IoT devices.
- *Susceptibility to Malware Infection and Other Abuse*: IoT devices are susceptible to malware and other abuses that can disrupt IoT device operations, gain unauthorized access, or launch attacks.
- *Potential for IoT Problems to Persist*: IoT security issues are likely to persist because the

devices may never be updated, and device replacement may be an alternative to software updates given that some IoT devices are inexpensive or even “disposable.”

Based on these observations, the Report concludes with a series of recommendations to address these privacy and security concerns with respect to IoT devices, including the following:

- *Use Best Current Software Practices*: IoT devices should ship with reasonably current software without severe known vulnerabilities and a mechanism for automatic, secure software updates.
- *Follow Security & Cryptography Best Practices*: IoT devices should employ cybersecurity best practices, including encryption, secure communications, and unique credentials for each device.
- *Function Without Internet Connectivity*: IoT devices should be able to perform primary functions (e.g., switching on lights or controlling thermostats) even if Internet connectivity or back-end cloud services are disrupted.
- *Clear Disclosures*: IoT devices should ship with an “easy to find and understand” privacy policy and clear consumer disclosures about device functionalities.
- *Industry-Wide Improvements*: The IoT device industry, manufacturer supply chains, and related consumer electronics groups should consider industry-wide cybersecurity programs.

National Law Review, Volume VI, Number 328