NEWSLETTER

Digital Security and Privacy Are Being Addressed Across the Federal Government

October 2016

Security and privacy are complementary concepts; without security, consumers cannot have privacy. Privacy and security—particularly in our increasingly connected economy—are complex and require agile responses and engaged consumers, who update their devices and use good cyber hygiene. Given the number of diverse global contributors to the tech sector, from OS providers to manufacturers, to application developers and network operators and end users, there is no single solution or approach.

Sweeping and difficult policy issues will not soon be resolved in Congress, but in the meantime, several activities are underway to address connectivity, security, and privacy in the digital ecosystem.

- The National Telecommunications and Information Administration (NTIA), located within the U.S. Department of Commerce, will address Internet of Things and consumer expectations about security in Austin, Texas on October 19, 2016. NTIA has convened a multistakeholder process concerning *Internet of Things Security Upgradability and Patching*. NTIA says that there has "sometimes been limited consideration for supporting future security patches, even though many devices will eventually need them," and "manufacturers can struggle to effectively communicate to consumers the security features of their devices." This process will consider how to develop a common lexicon or best practices. More information can be found here.
- The National Institute of Standards and Technology (NIST) is examining mobile threats and security across the federal government, creating a Mobile Threat Catalogue that purports

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Madeleine M. Lottenbach
Associate
202.719.4193
mlottenbach@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
Telecom, Media & Technology

to list varied threats across mobility. Some can be addressed through simple end-user cyber hygiene, while others require nation-state engagement to address global issues and trust. Comments are being taken and are due November 10, 2016. More information can be found here.

- NIST is looking at privacy controls and privacy risks associated with security controls. It proposes adding to existing security guidance "privacy considerations that are relevant to, or arise from, security controls." It is updating NIST Special Publication 800-53, Appendix J. NIST has held public workshops and the comment period closed on September 30, 2016. Information can be found here.
- NIST released on October 4, 2016, Special Publication 800-150, a Guide to Cyber Threat Information Sharing, which "provides guidelines for establishing and participating in cyber threat information sharing relationships. This guidance helps organizations establish information sharing goals, identify cyber threat information sources, scope information sharing activities, develop rules that control the publication and distribution of threat information, engage with existing sharing communities, and make effective use of threat information in support of the organization's overall cybersecurity practices." This publication addresses privacy and the potential impacts on privacy of various sharing activities.