

New Chamber White Paper on IoT Security

October 2017

Wiley Rein partner Megan Brown and several firm associates collaborated with the United States Chamber of Commerce to develop a white paper on security in the Internet of Things (IoT), with the goal of helping policymakers evaluate and consider whether and how to address privacy and security in the IoT. It highlights the incredible potential of the IoT for consumers and nations in the developed and developing world. We concluded that when it comes to security, attempts to regulate today may well be outdated tomorrow. Flexible approaches to collaboration and cooperation to address shared threats have significant advantages over national regulation, which may fragment the global economy. Ten key principles emerge from the report.

1. Any approach to IoT security should be data-driven, based on empirical evidence of a specific harm, and be adaptable both over time and cross-border.
2. Security demands should never be used as industrial policy to advance protectionism or favor national economic interests.
3. National boundaries need not become arbitrary obstacles to the movement of devices or data, or to the offering of IoT-related services.
4. Global standards work is the best way to promote common approaches and technology solutions. Such standards should be open, transparent, and technology-neutral.
5. Any government IoT strategy should promote technical compatibility and interoperability to the maximum extent possible.
6. Everybody is vulnerable, so cyber threats must be met with global information sharing and collaboration to improve and safeguard the IoT ecosystem.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

7. End users need to be educated about their roles and responsibilities in this digital age.
8. Manufacturers and vendors should be encouraged to routinely evaluate and improve endpoint security.
9. The international community must collectively condemn criminal activities that infect and exploit the openness and connectivity of the Internet and our digital future.
10. Governments must work together to shut down illegal activities and bring bad actors to justice