

## Senator discusses “asymmetrical threat” at ABA Internet of Things conference



Senator Mark Warner (D-VA) addresses The Internet of Things National Institute, sponsored by the ABA Section of Science and Technology Law

The Internet of Things (IoT) National Institute, sponsored by the [ABA Section of Science and Technology Law](#), attracted many business owners, lawyers and policy makers to its third annual meeting at the offices of Crowell & Moring LLP, May 9-10, in Washington, D.C.

Among these was keynote speaker Sen. Mark Warner (D-Va.), who discussed the potential vulnerabilities and advancements to be made with the nations’ use of IoT devices, along with cybersecurity.

“One area that is the lowest hanging fruit where the United States ought to move is on the question of Internet of Things,” Warner said. “I find it fundamentally bizarre where we live in a world where we have roughly about 10,000,000 IoT connected devices yet we have no minimum-security standards inside of IoT.”

IoT refers to computing devices that are interconnected via the internet and are embedded in everyday objects such as cars, thermostats and even hair dryers, which enable them to send and receive data. These IoT sensors constantly collect data, some of which can be very sensitive, such as collecting data from a usage patterns with an IoT-connected toy.

“One aspect of the low-hanging fruit around a cyber doctrine would be to say that the United States of America ought to at least, in terms of our tax dollars, make sure that when the federal government buys an IoT connected device, it has basic security built in,” says Warner.

The issue of security and privacy with IoT-connected devices poses a large risk for possible security breaches and privacy hacks.

“I believe the single largest threat we face in our nation right now is this asymmetrical threat posed by an ever-widening world of cyber vulnerabilities combined with these new tools of misinformation and disinformation in ways that we are not prepared for,” said Warner.

When asked by Jody Westby, CEO of Global Cyber Risk and the co-chair of ABA SciTech’s Privacy and Computer Crime Committee, his thoughts on supporting the establishment of a cyber committee on Capitol Hill to work on establishing safer security standards for IoT devices, Warner’s initial response

was yes. However, he raised the potential issue of trading cyber expertise for domain expertise, and said the goal would be to maintain both cyber and domain expertise simultaneously.

Working with the National Institute of Standards and Technology as well as industry standards, Warner encouraged the government to purchase IoT devices that can be updated and refrain from buying those that have fixed passcodes.

The two-day institute provided an opportunity for about 120 attendees to share knowledge and learn about issues and advancements surrounding IoT-connected devices as well as to voice concerns directly to policy makers on Capitol Hill.

Among the other speakers were U.S. Rep. Jerry McNerney (D-Calif.), who addressed IoT initiatives before Congress, and U.S. Rep. Robin Kelly (D-Ill.), who spoke on IoT oversight on Capitol Hill. Commissioner of the Federal Trade Commission Terrell P. McSweeney and the FTC's acting chief technologist, Neil Chilson, spoke about emerging security and privacy issues in a connected world.

This entry was posted on Mon May 14 15:23:12 CDT 2018 and filed under [Top Stories](#) and [Section of Science and Technology Law](#).