Is the IoT the End of Privacy As We Know It?

CITY OF PHILADELPHIA LAW DEPARTMENT JULY 25, 2019

Devin Chwastyk, J.D., CIPP/US, Member, Chair, Privacy & Data Security Group, McNees Wallace & Nurick LLC

<u>dchwastyk@mcneeslaw.com</u> <u>twitter.com/ChwastykD</u>



Overview of Topics

- 1. IoT regulatory landscape
 - A. Federal and state regulations
- 2. Regulatory enforcement actions
- 3. Regulatory challenges
- 4. Potential legal liabilities
- 5. A look into the future regulatory perspective



IoT Regulatory Landscape

- Security
- Privacy
- Frequency/spectrum management
- Certification



Security of the IoT

- Examples of IoT security issues
 - DDoS attacks

- Consequences of IoT security failures
- Obstacles to IoT security



Privacy and the IoT

- Facilitating communication between devices
- Obstacles to encryption and data protection
- New standards and philosophies for privacy and the IoT



Practical Regulations of the IoT

Frequency/Spectrum Management

Certifications



Federal Regulation of the IoT

- Federal Trade Commission
 - ASUSTeK Computer Inc.
 - D-Link Systems
 - Lenovo Group
 - Vizio
- COPPA compliance issues for children and toys
 - Vtech
- National Telecommuications and Information Association
- Pending federal legislation



State Regulation of the IoT

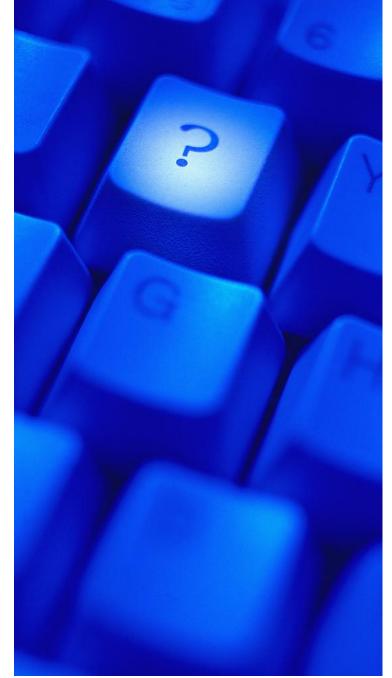
- California SB 327
- California Consumer Privacy Act
- Pending state laws
 - Pennsylvania?



The Future of Regulation and the IoT

- Potential regulatory liabilities
 - Device malfunctions
 - Cyberattacks and hacks
- The regulatory future for security, privacy and the internet of things
 - Unfair and deceptive practices
 - Minimization of vulnerabilities
 - Concreteness of alleged harms
 - Private causes of action







Questions?

Devin J. Chwastyk dchwastyk@mcneeslaw.com http://www.mcneeslaw.com twitter.com/ChwastykD

