Robinson+Cole

Who's in Charge of Regulating the Internet of Things?

KATHLEEN M. PORTER, ESQ.
SEPTEMBER 7, 2017

SCG LEGAL ANNUAL MEETING, DENVER 2017

Introduction

- The **'Internet of Things' (IoT)** is defined as:
  - Devices, sensors and electronics that connect, store, transmit and/or communicate data between or with each other via Internet, wireless or network
- Estimates are **20-30 billion everyday items by 2020** will be connected –in our homes, automobiles, food safety, medical devices, critical infrastructure, manufacturing, etc.

IoT ≠ Not the *Wild Wild West*

- Misconception that because data generated by IoT in a novel way, privacy, data security and other laws do not apply.

- Key for manufacturers to understand that **data generated by IoT is personal data**, sometimes very sensitive.

Robinson+Cole

IoT ≠ Not the *Wild Wild West*

- Statutes and regulations adopted during and prior to Internet age apply to IoT, even if by analogy.

- Enforcement actions by FTC and others also apply.

- Patchwork of federal, state and even industry guidance and legislation, particularly on disclosure, privacy, security, prohibition against unfair and deceptive practices.

SHERIFF

Robinson+Cole

IoT By Design

- Consider human impact IoT will have during product concept or **design process**.

- **Identify risks and vulnerabilities** so can take measures to mitigate them.

- **Data minimization**

- **Don't delay** until production or quality control phase or when begin marketing product.

Robinson+Cole

IoT Vulnerabilities

- Challenges on **vulnerabilities**
  - **Tension** between profit and speed to market v. cybersecurity
  - Patches and updates work for laptops and smartphones, but not with IoT devices. **Challenging to shut down** IoT device or whole internet-connected industrial facility or urban area

IoT Data Breach and Access

- **Unauthorized access** to personal data
- IoT used to **spread ransomware and malware and launch DoS attacks**
- **Data Requests** from law enforcement, government and private parties
- Potential **legal and public relations** issues

Robinson+Cole

IoT RoadMap to Privacy Policy and Terms of Service

- What Personal Data will IoT Service or Device Collect? Special protections
- How long will personal data be held?
- Who has administrative rights to access personal data?
- Who is hosting or sharing personal data? Third Party vendors?
- Draft Terms of Service
- Draft Privacy Policy to give notice that collecting Personal Data, include uses, storage, access and destruction
- Obtain consent before collect Personal Data (if possible)
- Honor ongoing rights with Respect to Personal Data
- Implement Reasonable Procedures to Protect Security of Personal Data
- Have Access Plan

Robinson+Cole

IoT Road Map to Privacy Policy and Terms of Service

- Make sure devices are not set to default (e.g. change passwords)
- Verify that all devices and sensors are managed and monitored
- Properly segment your network –create an internal, guest and IoT network at a minimum
- Update firewalls and review security configurations, including operating system updates and patches
- Secure remote access
- Require security software on every IoT device (and mobile devices connected to those IoT devices)
- Encrypt transmission and storage of data if possible
- Train employees

Robinson+Cole