Fox Rothschild LLP
ATTORNEYS AT LAW

# Privacy and the Internet of Things:

# Is the Internet of Things the End of Privacy as We Know It?

**Mark McCreary**

**Fox Rothschild LLP**

**Partner and Chief Privacy Officer**

# What is Internet of Things (IoT)?

- Internet + physical devices
- Convergence of multiple technologies into an ‘ecosystem’
- Concept of “smart devices”



| YEAR | NUMBER OF CONNECTED DEVICES |
|---|---|
| 1990 | 0.3 million |
| 1999 | 90.0 million |
| 2010 | 5.0 billion |
| 2013 | 9.0 billion |
| 2025 | 1.0 trillion |

# What is Internet of Things (IoT)?

- Smart home, wearables, connected car
- Smart cities: traffic, energy, crime
- Amazon Echo, Google Home

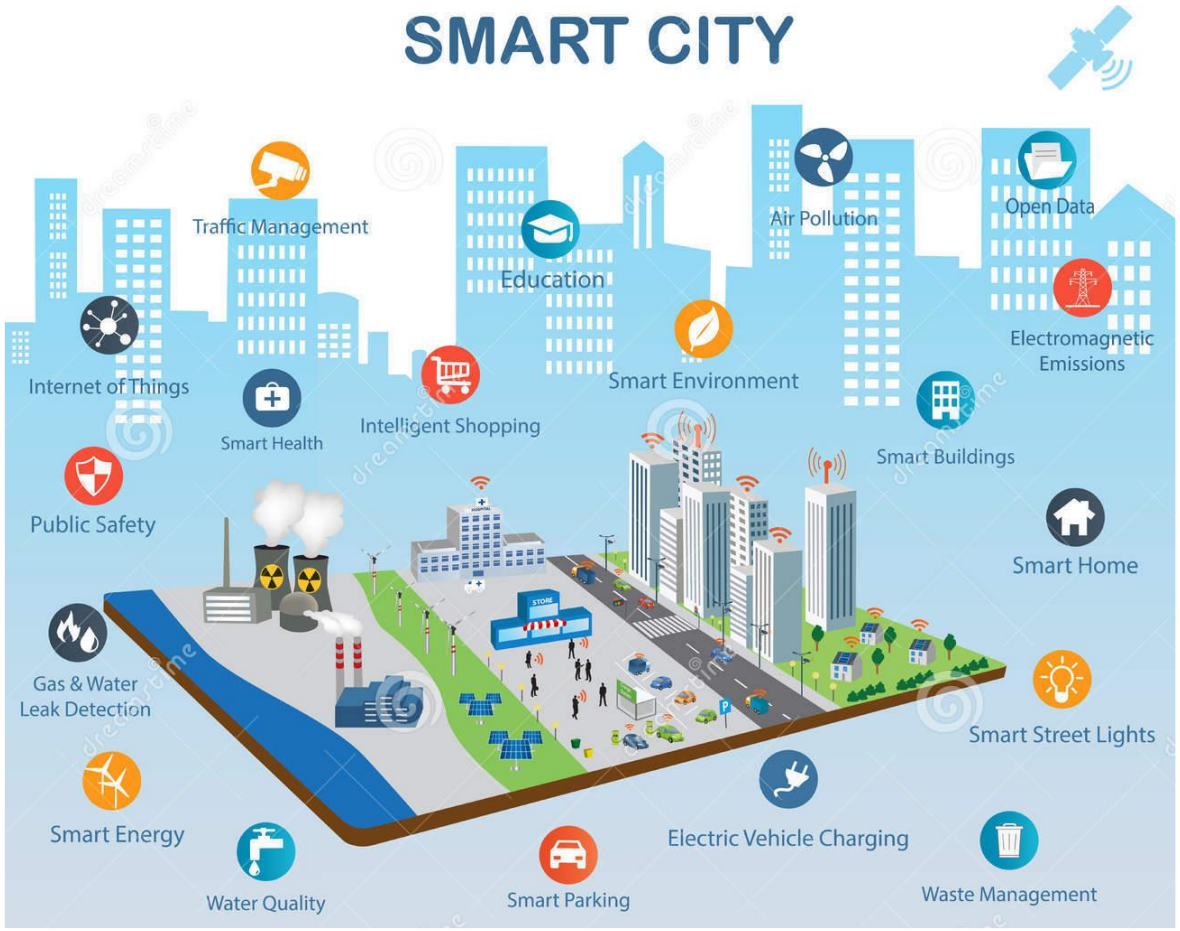
| Consumer | Enterprise and Industrial |
| --- | --- |
| smart speakers | worker productivity tracking devices |
| connected cars | smart office lighting |
| intelligent door locks | temperature-sensitive supply chain |
| fitness and health wearables | augmented reality maintenance equipment |
| smart lighting | autonomous trucking |
| networked thermostats | drones |
| smart TVs | disease management systems |
| robot vacuums | employee wellness trackers |
| internet-connected toys | automated retail checkout |
| networked bathroom appliances | inventory optimization sensors |
| indoor security systems | face recognition cameras for security |
| smart locks | building management sensors |

# Overview – Data Privacy and Compliance

- Benefits, but potentially greater privacy and security threats
- Traffic and transportation systems, power plants, water supply networks, waste management, crime detection, information systems, schools, libraries, hospitals, and other community services
- IoT Security Foundation provides compliance framework
- Relatively novel regulations

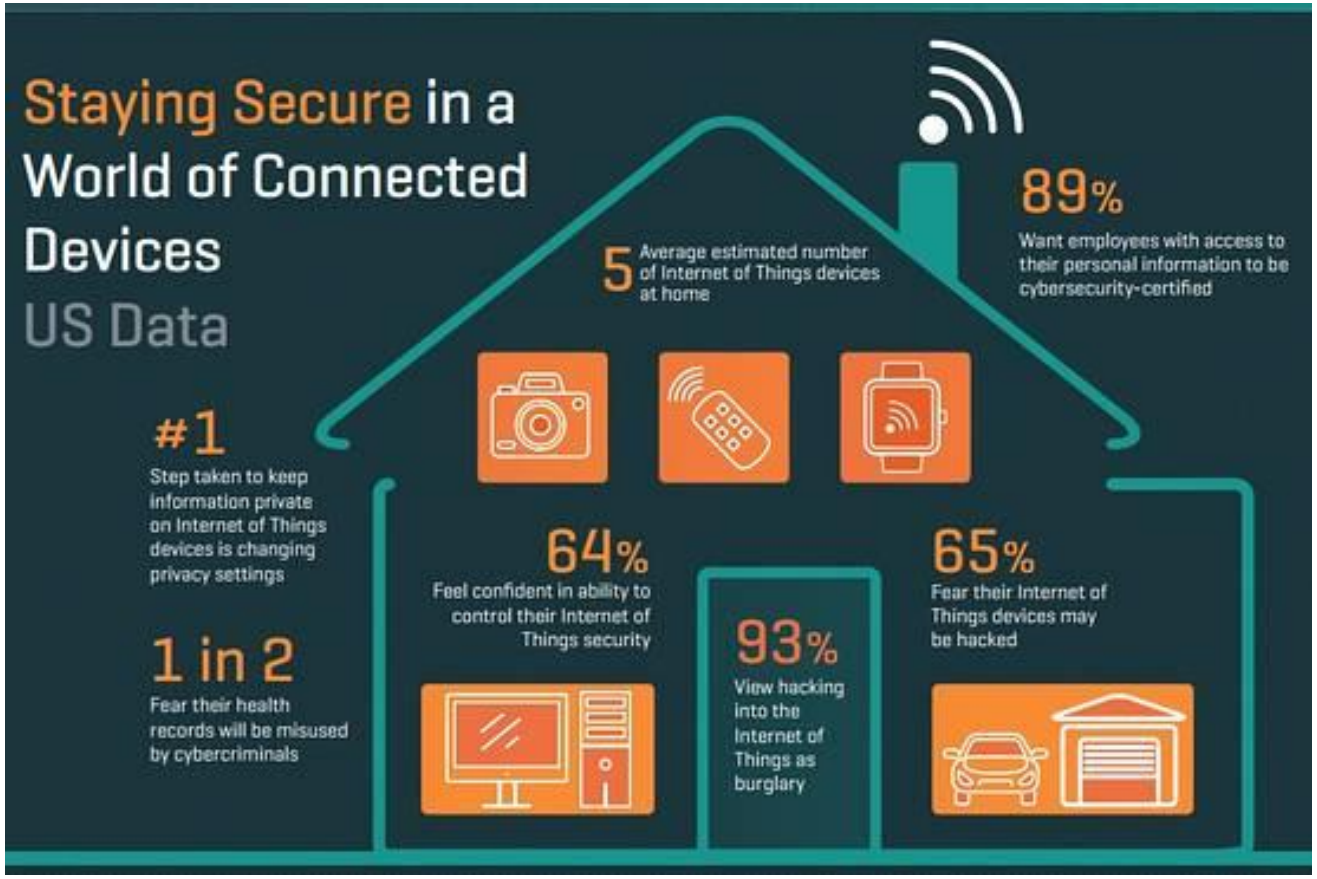
# Use, Sharing and Collection of Data

- Consumer Use
  - Fitbit, Apple HomeKit
- Commercial Use
  - Internet of Medical Things, Transportation
- Industrial Use
  - Manufacturing, Agriculture
- Municipal Use
  - Optimize the efficiency of city operations and services and connect to citizens



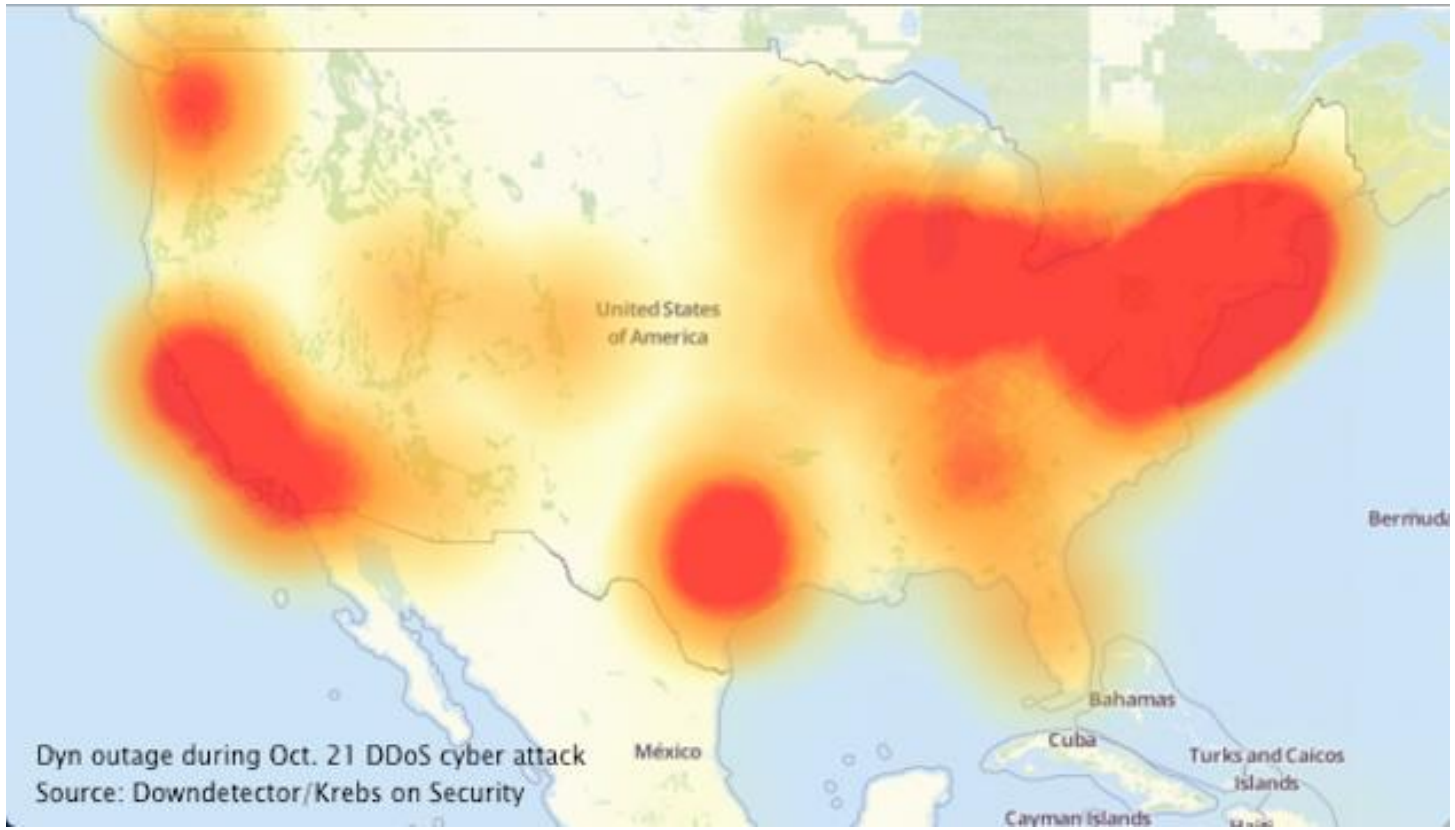
# Potential Challenges in Securing Devices

- With IoT, virtual threats become increasingly physical by targeting vulnerabilities
- Many IoT devices have operational and security restrictions because of their limited computational power



# Potential Challenges in Securing Devices

- October 21, 2016 Dyn Cyberattack – IoT focused malware disrupted major Internet platforms and services in Europe and North America
- Executed through a botnet using IoT devices, such as printers, IP cameras, residential gateways and baby monitors infected with the Mirai malware



# Major Privacy Issues

- Personal information such as online activities and lifestyle choices
- Household privacy can also be at risk, habits and patterns learned
- Lack of updates against vulnerabilities

# Privacy Policies

- There is little control over what is done with the data collected through IoT devices
- General lack of understanding what data is being collected, to what uses it is being put, with whom it is being shared
- Policies must explain how data is collected, used, and shared

> *"The IoT has the potential to really shift the home from a black box, what used to be a protective, safe space, to more of a glass house where everything that we do is now readily apparent to people who are willing to look for it."*
>
> *—Heather Patterson, Intel*[10]

# Privacy Policies and Safeguards

- California's SB-327
  - Starting on January 1st, 2020, any manufacturer of a device that connects "directly or indirectly" to the internet must equip it with "reasonable" security features, designed to prevent unauthorized access, modification, or information disclosure. If it can be accessed outside a local area network with a password, it needs to either come with a unique password for each device, or force users to set their own password the first time they connect. That means no more generic default credentials for a hacker to guess.

# Privacy Policies and Safeguards

IoT Cybersecurity Improvement Act

- By September 30, 2019, NIST must complete all ongoing efforts related to managing IoT cybersecurity, particularly its work in identifying cybersecurity capabilities for IoT devices. NIST must address at least: (i) secure development, (ii) identity management, (iii) patching, and (iv) configuration management for IoT devices.
- By March 31, 2020, NIST must develop recommendations on “the appropriate use and management” of IoT devices “owned or controlled by the Federal Government.” These include “minimum information security requirements” that address the cybersecurity risks of IoT devices owned or controlled by the federal government.

# Privacy Policies and Safeguards

- General Data Protection Regulation, oriented towards individuals' rights:
  - the right to know how data about you is processed (collected, analyzed, and used)
  - the right to object to such processing
  - the right to see the data that is stored about you
  - the right to a meaningful explanation about automatic data processing
  - the right to withdraw consent to processing
  - the right to have your data erased under certain conditions
  - the right be able to easily move your data from one provider to a different one