INTERNET OF THINGS: CONSUMER LANDSCAPE

Andrea Arias
October 19, 2017
Federal Trade Commission

The views expressed are those of the speaker and not necessarily those of the FTC or any one of its Commissioners.
FTC Background

- Independent law enforcement agency
- Consumer protection and competition mandate
- Privacy and data security are a consumer protection priority
  - Enforcement
  - Policy initiatives
  - Consumer education and business outreach
FTC Background

- **FTC Act** (15 U.S.C. §§ 41-58, as amended)
  - Prohibits unfair or deceptive acts or practices.
    - **Unfairness**
      - Acts or practices that cause or are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.
    - **Deception**
      - A material representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer’s detriment.
FTC Background

• **Children’s Online Privacy Protection Act of 1998 ("COPPA")**
  (15 U.S.C. §§ 6501-6506)
  • Protects children’s privacy.

• **Gramm-Leach-Bliley Act**
  • Protects consumers’ personal financial information.

• **Fair Credit Reporting Act**
  (15 U.S.C. §§ 1681-1681x, as amended)
  • Protects consumers’ information collected by reporting agencies, such as credit bureaus, for eligibility decisions.
FTC Privacy Cases
What is the “Internet of Things”? 

The Internet of Things “refers to ‘things,’ such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet.”
Consumer Benefits

- Healthcare
  - Reduce healthcare costs while giving consumers the ability to record, track, and monitor their own vital signs

- Home Automation
  - Greater energy efficiency and reduced costs

- Transportation
  - Safety and convenience benefits

- Societal Benefits
  - Aggregation of big data can lead to research and breakthroughs.
Consumer Risks: Privacy

- Direct collection of sensitive personal information

- Collection of personal information, habits, locations, and physical conditions over time, leading to inferences or unanticipated consequences

- Lack of consumer knowledge or consent

- Lack of accuracy of the data

- Amalgamation of various sources of data
Consumer Risks: Security

- Enabling unauthorized access and misuse of personal information
- Facilitating attacks on the consumer’s network or other systems
- Risks to personal and physical safety
Internet of Things: Privacy

User Experience Design

Many connected devices may not even have a traditional user interface, so companies must think holistically about the information and expectations that are conveyed through the broader user experience:

- Choices at point of sale
- Tutorials
- Codes on the device
- Choices during setup
- Management portals or dashboards
- Icons
- “Out of band” communications requested by consumers
- General privacy menus
- A user experience approach
Lessons Learned from FTC Cases

- Vizio: Deceptive User Interface Design
Internet of Things: Security

“The first step is remarkably hard: understanding that you have a problem. More precisely, it’s understanding that you’re in the networked software business, with all that implies, rather than in the phone, thermostat, printer, light bulb, or what have you business.”

Steve Bellovin, former FTC Chief Technologist, “Shipping Security”

- Is the software offered to consumers (e.g., device firmware, companion app, backend services) secure?

- Does it store data securely?
  - FTC Cases: Credit Karma, HTC America, TRENDnet

- Does it transmit data securely?
  - FTC Cases: Fandango, Credit Karma, TRENDnet

- Are the APIs secure?
  - FTC Case: Snapchat
Lessons Learned from FTC Cases

- TRENDnet: Lack of Security by Design

Direct Video Stream Authentication: Enable
Internet of Things: Security

“What will be the level of security and support [IoT devices receive] while under warranty? If a critical vulnerability is discovered, will an update be provided? What happens after the warranty expires? Should modern refrigerators have a shelf-life, much like the food contained within?”

Ashkan Soltani, Former FTC Chief Technologist, “What’s the security shelf-life of IoT?”

- Security is an Ongoing Process
  - IoT companies need to have a process for receiving, managing, and addressing security vulnerability reports
  - FTC Cases: *HTC America, Fandango*

- Security Updates and End-of-Life
  - Deploy and inform users about security updates
  - Informing consumers about minimum support periods and end-of-support
Welcome to IoT Watchdog

IoT Watchdog is a smartphone application which allows its users to simply and proactively manage their IoT devices with minimal effort.

What is IoT

The "Internet of Things" or "IoT", is the connection of devices which previously hadn't been connected.

Does it support Wi-Fi devices?

Yes.

What about Bluetooth devices?

Absolutely.

But I'm not technically minded!

That's certainly acceptable. IoT Watchdog was developed and tested with the mindset

Personal Assistant Devices

- Echo Dot, 2nd Gen, Black
  - Living Room

- DCS-932L Camera
  - Garage
FTC Resources


• Internet of Things Report
• Start with Security: A Guide for Business
• Careful Connections: Building Security in the Internet of Things
• Cross-Device Tracking Report
business.ftc.gov
Questions?

Andrea Arias
Federal Trade Commission
aarias@ftc.gov