Ransomware, Drones, Smart TVs, Bots: Protecting Consumers in the Age of IoT

Terrell McSweeny
Commissioner
Federal Trade Commission
@TMCsweenyFTC

Aaron Alva
Tech Policy Fellow
Federal Trade Commission
@aalvatar
Disclaimer

The views expressed do not necessarily reflect the views of the Commission or any individual Commissioner.
Why is the FTC in this space?

- Our consumer protection mission goes where consumers go
- Consumers are connected to the internet in more ways than ever
Why do we care about data security?

- Security concerns may be limiting adoption of new technologies, including IoT
- Different tools at our disposal
  - Law enforcement
  - Policy and research
  - Consumer and business education
Start With Security initiative

- 10 lessons learned from 60+ FTC data security cases
- Roadshow events in San Francisco, Austin, Seattle, Chicago
- ftc.gov/startwithsecurity
Data Security – Education

5. Segment your network and monitor who's trying to get in and out.

6. Secure remote access to your network.

7. Apply sound security practices when developing new products.

8. Make sure your service providers implement reasonable security measures.

9. Put procedures in place to keep your security current and address vulnerabilities that may arise.

10. Secure paper, physical media, and devices.
FTC’s law enforcement authority

- Protect consumers from unfair or deceptive acts or practices
  - Don’t lie
  - Don’t cause consumers unavoidable harm
IoT Security Cases

- ASUSTek – Routers
- TRENDnet – Connected security cameras
- D-Link – Routers and IP Cameras
Examples of security failures alleged by FTC

- Hard-coded/default login credentials
- Command injection vulnerabilities
- Exposure of private key
- Transmission or storage of login credentials in clear text
- Failure to perform security testing/reviews of software
Data Security – Research

- In-house research & investigations office – OTech. Recent research projects include:
  - Ransomware
  - Drones
  - Smart TVs
  - Ad preferences based on social networks
  - Cross Device Tracking
Some research topics we’re interested in

- Understanding and quantifying privacy and security
  - How companies assess & manage security risks
  - Ways consumers are impacted by breaches
  - Security attack trends & mitigations

- Emerging technologies

- Tools & techniques
  - Automated tools to understand data collection/sharing practices and detect fraud, etc.
IoT Security – Reports

IoT Staff Report – Jan. 2015

- Risk of DDoS attacks from insecure IoT devices

- Staff Guidance
  - Should implement security by design
  - Should incorporate smart defaults, incl. requiring changing default passwords
  - Should test devices before release
  - Should patch devices
Other Reports

Recent/New
- Big Data
- Cross-Device Tracking
- Annual Privacy & Data Security Update

Upcoming
- Mobile security updates study
  - Update process
  - Vulnerability response
  - Testing
  - Third-party oversight
- PCI DSS audit study
  - Compliance Assessment
  - Data Security Forensic Audits
Competition to create a technical tool that consumers can use to guard against security vulnerabilities & ensure IoT devices are up-to-date

- Entries due May 22, 2017
- [https://www.ftc.gov/iot-home-inspector-challenge](https://www.ftc.gov/iot-home-inspector-challenge)
Apply – How you can help promote innovation & consumer welfare
Apply – How you can help

- Directly with FTC
  - Share research with us ➔ research@ftc.gov
  - Participate in challenge, workshops
Apply – How you can help

With your company

- Apply **Start with Security** principles
- Promote culture of data security, bringing security to the forefront throughout all departments and all levels of your company
Summary

- FTC is active on data security and IoT security issues
- Start with Security initiative resources available to help startups & small businesses with basic security considerations
- FTC’s in-house research helps understand emerging technology & aids with technical investigations
- Challenge hopes to boost IoT security for consumers