Internet of Things – The Latest Frontier (Part 2)
A talk with John Heitmann and Jameson Dempsey

I. Security

A. Security risks in IoT

1. Because IoT devices are interconnected and operate as part of a system, a security vulnerability in one part of the chain may expose others in the system. Any IoT device can potentially be hacked.
2. Data breaches can result from lack of encryption, poor web interface security, insecure update mechanisms, or even the use of simple passwords or human error.
3. Security breaches can also pose risks to physical safety. For example, devices like smart-cars, insulin pumps, or home security systems can be hacked and used to harm the consumer.
4. Often, many new entrants to the IoT market are not experienced in dealing with these issues, and data security is an afterthought.

B. Breaches and FCC enforcement

1. Cox Communications security breach and FCC enforcement
   a. In August 2014, Cox Communications security was compromised when a hacker, part of the "Lizard Squad" hacker group, successfully gained access to Cox internal databases by sending a Cox employee a phishing link and gaining their login credentials. The hacker accessed Cox cable customers' personal information, including names, addresses, email addresses, secret questions and answers, PIN, and some partial Social Security numbers, and posted them online.
   b. Cox did not inform all 61 customers who were affected by the breach and did not report the breach to FCC as required by law.
   c. The FCC ordered Cox Communications to pay a $595,000 civil penalty to settle an investigation into whether Fox failed to properly protects customers' personal information when security was breached.[1] In addition, Cox was required to identify and notify all affected customers and provide them with one year of credit monitoring. As part of the settlement, Cox was also required to implement a compliance plan that includes annual system audits, internal threat monitoring, penetration testing, and additional breach notification systems and processes.

C. FCC recommendations for best practices[2]

1. Implement security by design by building security into devices at the outset. Do a privacy or security risk assessment of the consumer information collected and retained. Consider data minimization. Test security measures before launching product.

[1] FCC Press release for Cox Communications consent decree, Nov 5, 2015: https://www.fcc.gov/document/cox-communications-pay-595000-settle-data-breach-investigation-0

[2] FTC Report on Nov 2013 Workshop, Internet of Things: Privacy and Security in a Connected World: https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

2. Train employees about good security practices.
3. Retain service providers capable of maintaining reasonable security.
4. Implement a defense-in-depth approach, considering security measures at several levels.
5. Consider implementing reasonable access control measures to limit ability of an unauthorized person to access a consumer's device, data, or network.
6. Monitor the device throughout the life cycle and patch known vulnerabilities.

II. Net Neutrality

A. What is net neutrality
  1. Concept of keeping the Internet open and that all internet traffic should be treated equally. Meaning that Internet service providers should enable open networks and not block or discriminate against certain applications or content.
  2. Proponents argue that prioritized internet allow for unfair competition.
  3. Opponents argue that government control stifles creativity and that high priority services like health care should have priority bandwidth over lower priority services.

B. *Caterfone* and consumer choice
  1. *In re Use of the Carterfone Device*, 13 F.C.C.2d 420 (June 26, 1968)
     a. AT&T essentially operated a monopoly over the nation-wide telephone network. It controlled access to its network through its foreign attachment provisions and tariffs which prevented any equipment or device from being attached to its network without its permission.
     b. The FCC determined that foreign devices could be attached to the public telephone network so long as the devices were privately beneficial and not publicly harmful. It found AT&T's tariff unreasonable because it prevents use of harmful and harmless devices.
  2. *Carterfone* allowed consumers to have a choice in telephone equipment and functions other than those made by AT&T. It's often credited as enabling the development of the Internet.

C. FCC's 2015 Open Internet Order[3]
  1. In 2015, FCC issued an order to reclassify broadband as a "telecommunications service," as defined under Title II of the Communications Act, to enforce net neutrality and prohibit throttling or content blocking.
  2. The Order prohibits the following:
     a. Blocking of lawful content, applications, or services;
     b. Throttling or slowing down specific content, applications, or services
     c. Paid prioritization or accepting fees for priority treatment.

D. New rules in effect
  1. *In the Matter of AT&T Mobility, LLC*[4]

[3] FCC Open Internet Order and Rules: https://www.fcc.gov/general/open-internet

[4] FCC Notice of Apparent Liability for Forfeiture and Order, In the Matter of AT&T Mobility, LLC: https://www.fcc.gov/document/att-mobility-faces-100m-fine-misleading-consumers

a. FCC proposed a $100 million fine to AT&T for its allegedly misleading its customers who had unlimited data plans throttling service when customers had used a certain amount of data without disclosing that it was doing so. FCC determined that AT&T's use of "unlimited" to describe a data plan when it fact the service was subject to speed reductions after reaching a data threshold was misleading and that AT&T had failed to disclose the speed reductions.

b. FCC cited its 2010 Open Internet Transparency Rule, which mandates that broadband access providers disclose accurate and sufficient information for consumers to make informed choices.

III. Future of IoT

A. Growth of IoT necessitates forward thinking measures and laws

1. Surge in IoT devices will dramatically alter our lives.
2. For IoT to reach its full potential, both consumers and businesses need to understand the risks in big data and institute measures to standardize privacy and security.
    a. Companies have to take into account security measures at the outset and be aware of the privacy issues that may arise from the type and amount of information they are collecting. Implement privacy and security by design.
    b. Consumers need to make sure they understand what information they are sharing.
3. Data minimization
    a. Concept of limiting the data that companies collect and retain, and disposing of the information once no longer needed.
    b. Unique challenge in IoT in that it can be difficult at the outset to determine what types of data are beneficial and what should be minimized.
    c. Is a consideration that should be integral to privacy and security by design.

B. Future of IoT legislation

1. FTC recommends that IoT-specific-legislation is premature at this stage. FTC believes Congress should enact data security and privacy legislature to protect consumer data and consumer choice.
2. Laws relating to data privacy and security will likely develop incrementally
3. Currently, no IoT-specific-legislation pending in Congress