Internet of Things – The Latest Frontier (Part 1)
A talk with John Heitmann and Jameson Dempsey

I. What is the Internet of Things

A. Internet of Things (IoT)
   1. Not one widely accepted definition of IoT. Generally, an ecosystem of physical objects connected to the internet. Commonplace and everyday objects collect data and communicate to other devices and parties.
      a. E.g. cell phones, wearable technology, watches, headphones.
      b. E.g. Nest – a smart thermostat that uses sensors, activity in the home, and weather forecasts to adjust the temperature while maximizing energy efficiency.
      c. E.g. Fitbit – a health monitoring device that pairs with a smartphone to track the wearer's movements and physical activity.
   2. IoT wide reach and range of "things"
      a. In the near future, every object that can be connected will likely be connected.
      b. By some accounts, IoT related consumer spending is estimated to reach over $2.6 trillion by 2020.
      c. Affects a wide range of sectors and products: health and medicine, homes, cars, energy, electronics, transportation systems, etc.
      d. Will have deep impact on how consumers interact with and incorporate technology into daily lives.
   3. Potential benefits
      a. Examples of IoT uses:
         i. E.g. Home automations systems that allow users to not only set temperature control prior to returning home but play music, heat up coffee, turn on the vacuum, etc.
         ii. E.g. Pacemakers that would alert the doctor or hospital.
         iii. E.g. Insulin pumps that allow the user to track and monitor their vital signs.
      b. Ease and improve quality of everyday life.
      c. Empower users to make better decisions about consumption of things like electricity, energy, fuel, etc.
      d. Potential increase safety benefits for things like connected cars.

B. Issues in IoT
   1. Privacy
   2. Security
   3. Net neutrality

C. Federal agencies
   1. Federal Trade Commission (FTC) – oversees consumer protection.
      a. Federal Trade Commission Act empowers the FTC to regulate methods of competition and prohibit unfair and deceptive practices that affect commerce.
   2. Federal Communications Commission (FCC) – regulates interstate and international communications via radio, television, wire, etc.

II. Privacy

A. U.S. privacy laws
   1. No omnibus privacy law in the U.S.
      a. Privacy Act of 1974 provides safeguards against invasion of personal privacy through the misuse of records by Federal Agencies. [1]
      b. Health Insurance Portability and Accountability Act (HIPAA) may apply for health related devices. [2]
      c. Children's Online Privacy Protection Act (COPPA) may apply if the user is a child under 13 years of age. [3]
      d. Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999 may apply if the business is a financial institution.[4] Requires them to explain their information-sharing practices and to safeguard sensitive data.
   2. Data privacy laws applicable to IoT vary state by state. Not all states have laws regarding data disposal, data security breach, or internet privacy laws.
      a. Among the states, California has the most robust digital privacy laws.
         i. Was one of the first to provide an express with of privacy in its constitution and the first to have a notification requirement for security breaches.
         ii. California's Online Privacy Protection Act of 2003[5] – requires online services and websites that collect personal information to have a privacy policy with enumerated terms and to comply with that policy.
         iii. Among its many other privacy laws, includes laws that requires businesses that maintain personal information to adopt and implement reasonable security measures; stringent disclosure requirements on how parties collect personally identifiable information relating to consumers' online activities; laws relating to mobile app privacy policies

B. What data is being collected and how is it being used?
   1. More data given means less privacy. Consumers are willingly giving certain information but oftentimes, they are not aware exactly what information is collected and how it may be disseminated.
   2. Individuals may operate under the assumption that they own their own data but that is mostly not the case. For the privilege of or agreement to using the product, they

---

[1] Privacy Act of 1974: https://foia.state.gov/Learn/PrivacyAct.aspx
[2] The HIPAA Privacy Rule : http://www.hhs.gov/hipaa/for-professionals/privacy/
[3] COPPA: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
[4] Gramm-Leach-Bliley Act: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act
[5] Online Privacy Protection Act of 2003 - Online Privacy Protection Act of 2003 - California Business and Professions Code sections 22575-22579: http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article=

are giving up their privacy rights to that information. The information could be freely traded and shared with other parties.

3. Devices may collect personally identifiable information as well as non-personally identifiable information, and may collect that information directly or indirectly.
    a. Even if not personally identifiable information, can still be sensitive information that relate to health or geo-location information.
    b. Personal information like habits or geo-location information, if collected over time, can reveal a lot about a particular individual.

C. Privacy policies and terms of use
1. As IoT grows, becomes more crucial that consumers understand what is contained in privacy policies and terms of use agreements.
    a. As it stands now, privacy policies and terms of use are notoriously dense and rarely read in entirety by consumers. Important for businesses to draft policies that may be easily understood.
    b. Consequences of poorly drafted privacy policies - businesses can be sued for fraud and deceptive business practices, breach of contract, breach of good faith and fair dealing, breach of implied warranty, or negligence.
2. When crafting policies
    a. Questions to ask:
        i. What is the information being collected
        ii. How is the information being collected
        iii. How is the data being stored
        iv. How is the data being shared
    b. Importance of disclosure and transparency
        i. Explaining to the consumer how the information is generated by the device is crucial but an oft overlooked step, especially when many of these IoT devices do not have a keyboard or interface so are seemingly not collecting personally identifiable information.
3. FTC Report on Internet of Things recommends that companies notify users and give them choices about how the information is used. The FTC recognizes that there is no one-size-fits all approach and offers many ways to provide notice and choice, including:
    a. Choices at points of sale: opt-in multi-level choices at time of sale
    b. Tutorials that guide consumers through the company's privacy policy
    c. QR codes for devices without interfaces that could be scanned to take the consumer to a website that lays out the privacy and terms of use
    d. Set-up wizard that provides privacy choices
    e. Privacy dashboards that allow the consumer to configure and revisit
    f. Icons that quickly convey settings and attributes.
    g. See more here: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

III. 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. Telecommunications Act of 1996[6]
   1. Amended the Communications Act of 1934[7] which combined federal regulation of the telephone, telegraph, and radio communications and created the FCC to regulate these areas.
      a. Title II of the Communications Act defines "utility" as a local exchange carrier or public utility who owns or controls, in whole or in part, for any wire communications.
      b. "Common carrier" is defined as any common carrier engaged in interstate communication by wire or radio.

C. Verizon v. Federal Communications Commission[8]
   1. In 2010, the FCC issued its Open Internet Order, requiring transparency in terms of service, prohibiting blocking, and prohibiting discrimination in network traffic. Verizon filed suit challenging the Order on several grounds, including FCC's lack of statutory authority and that the rules violated the Communications Act which prohibit the FCC from regulating broadband providers in contrast to how other telecommunications providers are regulated.
   2. The D.C. Circuit held that FCC had authority to enact the rules but that it had regulated broadband providers as common carriers despite not classifying them as such in violation of the Communications Act. It vacated the rules that prohibited blocking and discrimination.

---

[6] Telecommunications Act of 1996: https://www.fcc.gov/general/telecommunications-act-1996
[7] Communications Act of 1934: https://www.fcc.gov/Reports/1934new.pdf
[8] 740 F.3d 623 (D.C. Cir. 2014): http://www.cadc.uscourts.gov/internet/opinions.nsf/3AF8B4D938CDEEA685257C6000532062/$file/11-1355-1474943.pdf