Privacy as a Differentiator in the Consumer Market
- Forrester Research predicts that privacy will become a competitive differentiator in 2015
  o Report predicts that making empty statements will not be sufficient
  o Companies will need to:
    ▪ 1) follow through with appropriate privacy policies
    ▪ 2) means of enforcement, and
    ▪ 3) building privacy considerations into business operations and the products or services offered to customers.
  o Developing corporate privacy consciousness will require the leadership of a Chief Privacy Officer, Data Protection Officer, or privacy professional to take on this responsibility to rally and oversee privacy efforts.
  o Forrester expects half of enterprises to see privacy as a differentiator by the end of 2015.
  o Reasons for the shifting trend:
    ▪ 1) Encryption and key management will become critical to prevent growing instances of cybercrime
    ▪ 2) Security and privacy professionals are increasingly using rights management tools to “place controls closer to the data itself and gather intelligence (e.g., real-time analytics and contextual information) about how the data is used”
    ▪ 3) Data disposal is gaining increasing attention
    ▪ 4) Social media adoption is increasing necessitating increased privacy controls
    ▪ 5) Increased use of wearables collecting Personal Health Information (PHI)

Wearable Technology and Privacy
- Research on the Internet of Things performed by TRUSTe shows:
  o 35% of Americans own at least one smart device other than a phone
  o 79% of US consumers are concerned about their personal information collected by smart devices
  o 69% believe they should own the personal data collected by using their smart devices
  o Primary consumer concerns:
    ▪ 87% said use and control of their personal data with the highest concern being personal information collected and used in ways they were unaware
    ▪ 86% said identity theft
    ▪ 86% are concerned that their device would be infected by malware
    ▪ 78% are concerned that their location might be revealed without their knowledge
- Edith Ramirez (Chairwoman, FTC) @ Consumer Electronics Show, Jan 2015
  o Three primary concerns
- (1) ubiquitous data collection of personal information, habits, location, and physical condition;
- (2) the potential for unexpected uses of consumer data that could have adverse consequences; and
- (3) heightened security risks, such as:
  - Relative small size and sophistication of IoT device manufacturers;
  - small size and limited processing power of many connected devices, resulting in an inability to encrypt data

  “Three Key Steps...to enhance consumer privacy and security and thereby build consumer trust in IoT devices”:
  - (1) adopting “security by design”, such as by;
    - conducting security audits early in product development
    - smart defaults (e.g., require password change)
    - encrypting storage and transmission of sensitive data (e.g., Personal Health Information)
  - (2) engaging in data minimization; and
  - (3) increasing transparency and providing consumers with notice and choice for unexpected data uses.

**FTC Attempts to Regulate Big Data**

- Edith Ramirez (Chairwoman, FTC) FTC Roundtable, Sept 2014
  - By raising awareness of the risks presented by big data, the FTC hopes it can become a tool for economic inclusion, not exclusion
- FTC Big Data Report to the Obama Administration, May 2014
  - Recommends the passage of data breach legislation that would create a single, national data breach reporting standard.
  - Warns that online data gathered on students, such as educational data, needs a higher federal standard of protection.
- Recent FTC Enforcement Actions:
  - Credit Karma and Fandango
    - Settled claims that these mobile apps’ security enabled consumers’ sensitive personal information, including credit card information and Social Security numbers to be vulnerable to interception.
    - Settlement required the companies to establish “comprehensive security programs designed to address security risks during the development of their applications and to undergo independent security assessments”
  - Snapchat
    - Settled charges Snapchat deceived consumers with claims about how their picture messages disappeared once sent through Snapchat servers, the amount of personal data collected, and the security measures taken to protect that data from misuse and unauthorized disclosure.
• Requires Snapchat will be required to implement a comprehensive privacy program that will be monitored by an independent privacy professional for the next 20 years.

- APEC Cross-Border Privacy Rules (CBPRs)
  o Self-regulatory scheme from the transfer of Personal Information between Asia-Pacific region countries
  o 25 Data Protection Authorities from APEC economies have signed on to enforce the APEC Cross-border Privacy Enforcement Arrangement
  o FTC is the biggest driver for the United States’ involvement in the APEC Privacy Framework.
    • Enforces CBPRs with §5 of the FTC Act (deceptive practices) as a company that chooses to participate in the CBPRs makes a public commitment to abide by the program requirements.