Government surveillance

Lorrie Faith Cranor
November 5, 2015

8-533 / 8-733 / 19-608 / 95-818:
Privacy Policy, Law, and Technology
Today’s agenda

• Quiz
• Homework discussion
• Surveillance
• Videos!
Homework discussion

• Select one technology you saw in the biometrics lab
  – How is this biometric used for identification and/or authentication
  – Describe two specific applications for which this biometric is currently used
  – Does this technology raise privacy concerns, or does it address privacy concerns?

• What data collection is facilitated by sensors, beacons, and other devices found in public spaces in NSH?
  – Where are they?
  – What data is being collected and what is it used for?
  – How could people who spend time in NSH be notified?
Homework discussion

• Which location technologies work by receiving transmissions to the device without sending any signals from the device?
  – If the smartphone does not send signals to get the location why there could still be privacy concerns.

• Elsa sees an ad for silver gloves with red rubies on her Facebook page, just the day after she browsed on-line shops for silver gloves with red rubies. Describe and draw a simple diagram illustrating the mechanisms used to provide this ad to her.
By the end of class you will be able to:

• Be familiar with a variety of US government surveillance programs and the privacy concerns that they raise
Surveillance systems you should know about

• Clipper chip
• Echelon
• TIA
• Carnivore
• CALEA
• MATRIX
• PRISM
Clipper chip

• 1993-1996

• Chipset developed by NSA for encrypting telephone conversations

• Secret “Skipjack” algorithm developed by NSA used “key escrow”
  – Strength of encryption algorithm could not be publicly evaluated
  – Foreign countries would not want their keys escrowed by US gov

• Serious vulnerability pointed out by Matt Blaze
  – Relied on 16-bit hash that could be quickly brute-forced to substitute non-escrowed key, disabling the key escrow
Echelon

- Signals Intelligence (SIGINT) collection and analysis networked operated by Australia, Canada, New Zealand, UK, and US
- Created for military/diplomatic Cold War monitoring, but evolved to monitoring civilians
- Intercepted phone calls, fax, email, etc.
- Uses satellite interception, undersea cables, microwave transmission
- Has list of keywords that are searched for automatically in intercepted messages
Total Information Awareness

- DARPA 2002-2003
Carnivore

- 1997-2005
- FBI system to monitor electronic communication
- Custom packet sniffer to monitor Internet traffic
- Physically located at an ISP or other network
- Required used of custom filters
- Lots of secret details, requires trust that it is legal
CALEA

- Communications Assistance for Law Enforcement Act
- US wiretapping law passed in 1994
- Required telecom carriers and manufacturers to modify their equipment and facilities to allow law-enforcement surveillance
- 2004 FCC expands CALEA to include some Internet communications (broadband, VoIP)
- 2013 and beyond – FBI pushing for CALEA to apply to all Internet communications and force all companies to add backdoors for government
PRISM

• NSA surveillance program operated since 2007
• Collects Internet communications, including encrypted communications
  – Foreign targets and US targets with a warrant
• Many technology companies are participants including Microsoft, Yahoo!, Google, Facebook, YouTube, AOL, Skype, Apple
• Publically revealed by Edward Snowden in 2013
Video

• http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet?language=en
Discussion

- Why do people care?
- Why does this matter?
- What can people do to protect themselves?