

# Government surveillance

Lorrie Faith Cranor

November 26, 2013

8-533 / 8-733 / 19-608 / 95-818:  
*Privacy Policy, Law, and Technology*

**Carnegie  
Mellon  
University**

CyLab



Engineering &  
Public Policy



# 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

# PRISM

- NSA surveillance program operated since 2007
- Collects Internet communications, including encrypted communications
- Many technology companies are participants including Microsoft, Yahoo!, Google, Facebook, YouTube, AOL, Skype, Apple
- Publically revealed by Edward Snowden in 2013



# Discussion

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



**Carnegie Mellon University**  
CyLab



Engineering &  
Public Policy