Lecture 6-1
Privacy and the Government

Addison-Wesley
is an imprint of
PEARSON

Participation Quiz

Do you think there should be more women in Computer Science?

a) No, I think things are right the way they are
b) Meh, I don't really care
c) Yes, but I don’t think much can be done about it
d) Yes, and I think we should do something about it

Solove's Taxonomy of Privacy

Privacy can become an issue in four different ways:

- **Information collection:** gathering personal information
  - "How much information do I have to give to rent a car?"
- **Information processing:** storing, manipulating, and using information that has been collected
  - "Should Google use the content of my emails to target ads?"
- **Information dissemination:** spreading personal info
  - "Is it wrong to forward an email that was sent to me?"
- **Invasion:** intruding upon a person's daily life
  - "Is it a good idea to email professors you might be interested in working with in grad school? How many: 2, 10, 100, 1000?"

Strong Encryption

- Strong encryption: encryption at a level that is believed not to be breakable by any other than sender/receiver
  - e.g., 256-bit AES
  - mathematical reasons to believe governments can't break it either
- Availability of strong encryption
  - Previously classified as a munition by US, regulated
  - 1991: US Senate passed a law requiring all encryption systems to include a "back door"
  - In response, Phil Zimmerman created PGP
  - Government tried to shut it down
  - 1999, 2000: courts ruled that these restrictions are illegal, encryption protects privacy and free speech
- *Questions*
  - *Should there be laws against use/distribution of strong encryption?*
  - *How should governments respond to its existence?*

USA PATRIOT Act (2001; 2011)

- Provisions
  - Greater authority for intelligence agencies to monitor communications within USA
  - Greater powers to regulate banks to prevent money laundering, particularly involving foreigners
  - Greater border controls
  - New crimes and penalties for terrorist activity, including indefinite detention of foreigners
  - Terrorism redefined to include domestic terrorism
- Critics say Act undermines 4th Amendment rights
  - Searches (of phone, internet, financial records) and seizures without warrants
  - Warrants issued without need for showing probable cause

Wiretapping in the Digital Age

- Carnivore Surveillance System
  - Created by FBI in late 1990s
  - Monitored Internet traffic, including email exchanges
  - Captured packets going to/from a particular IP address
  - Used about 25 times between 1998 and 2000
- Post 9/11:
  - Bush authorized new, secret, intelligence-gathering operations inside United States
    - OK for NSA to intercept international phone calls & emails initiated by people inside U.S.; no search warrant required
  - Monitored ~500 people inside U.S.; 5000-7000 people outside
  - Two al-Qaeda plots foiled
    - Plot to take down Brooklyn bridge
    - Plot to bomb British pubs and train stations

Snowden and the NSA Scandal

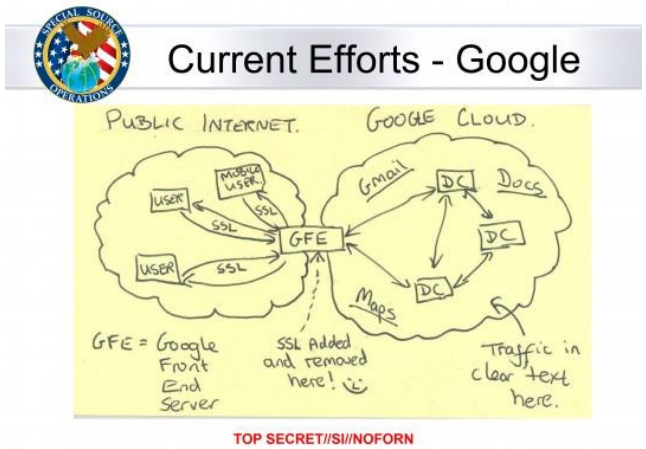
In the fall of 2013, it has emerged that the NSA has been engaged in a very wide range of wiretapping activities.

Which ones can you list?

What do you think about wiretapping more broadly?

Do you think Snowden behaved unethically?

TOP SECRET//SI//NOFORN



TOP SECRET//SI//NOFORN

Bill C-30

- "Protecting Children from Internet Predators Act"
  - Originally titled "Lawful Access Act"
- Proposed on February 14, 2012
- Key elements:
  - Requiring internet service providers to give subscriber data to police and national security agencies without a warrant, including names, unlisted phone numbers and IP addresses.
  - Forcing internet providers and other makers of technology to provide a "back door" to make communications accessible to police.
  - Allowing police to seek warrants to obtain information transmitted over the internet and data related to its transmission, including locations of individuals and transactions.
  - Allowing courts to compel other parties to preserve electronic evidence.
- After much public debate and controversy, quietly withdrawn by the Conservatives in the summer of 2012

Privacy and the Government

"The government should do all that it can to maintain the capability to intercept all encrypted communications."