CS 4001: Computing, Society & Professionalism

Munmun De Choudhury | Assistant Professor | School of Interactive Computing

Week 9: The Patriot Act/Privacy and the Government
March 5, 2019

Some reminders and updates

- Midterm on Thursday
- Makeup midterm exams next week
  - Please email me by Friday EOB to schedule your makeup exam
- Homework 3 released
  - Due in two weeks
- Grading update
- Quiz 2 today!

6.5 US Legislation Authorizing Wiretapping

Title III

- Part of Omnibus Crime Control and Safe Streets Act of 1968
- Allows a police agency with a court order to tap a phone for up to 30 days
- In 1972 US Supreme Court again rejected warrantless wiretapping, even for national security

Electronic Communications Privacy Act

- Passed by Congress in 1986
- Allows police to attach two kinds of surveillance devices to a suspect's phone line
  - Pen register: displays number being dialed
  - Trap-and-trace device: displays caller's phone number
- Court order needed, but prosecutors do not need to show probable cause
- Allows police to do roving wiretaps (following suspect from phone to phone)

Stored Communications Act

- Part of Electronic Communications Privacy Act
- Government does not need a search warrant to obtain from an Internet service provider email messages more than 180 days old
- Advent of cloud computing raises new privacy concerns
- Digital Due Process organization (nearly 50 companies and privacy rights organizations) lobbying Congress to change law

Foreign Intelligence Surveillance Act

- FISA provides judicial and congressional oversight of covert surveillance of foreign governments and agents
- Allows electronic surveillance of foreign nationals for up to one year without a court order
- Amended in 2007 to allow government to wiretap communications to/from foreign countries without oversight by FISA Court

6.6 USA PATRIOT Act

The USA Patriot Act

- Formal definition: the Uniting and Strengthening America by Providing Tools Required To Intercept and Obstruct Terrorism (USAPA)

Terrorism In the U.S.

- Domestic vs. International terrorism
- The need to fight terrorism
- Relation to computing
- The government's solution

Definition of Terrorism

- FBI defines terrorism as “the unlawful use of force or violence against persons or property to intimidate or coerce a government or civilian population”

Definition of Terrorism

- The Patriot Act defines terrorism differently.
- Expands notion of “domestic terrorism”
- Amends Computer Fraud and Abuse Act by stating that computer crimes are “terrorist offenses”

Some of the Major Provisions

- Court subpoena no longer needed for ISP's to give information
- Computer crimes are now "terrorist" offenses
- ISP's have to give up more user information
- Court orders no longer needed for monitoring suspects in computer crimes cases
- Appends the Computer Fraud and Abuse Act
- Major changes at Libraries in the U.S.
- Development of electronic crime task force within the U.S. Secret Service
- Implementation of the Carnivore Tracking Device – a customizable packet sniffer that can monitor all of a target user's Internet traffic

National Security Letters

- FBI can collect Internet, business, medical, educational, library, and church/mosque/ synagogue records without showing probable cause
- Issues a National Security Letter stating the records are related to an ongoing investigation; no approval from judge needed
- Gag orders prevent recipients (e.g., libraries) from disclosing receipt
- FBI issued 50,000 National Security Letters a year between 2003 and 2006

Analysis of the USAPA by President Bush

"Surveillance of communications is an essential tool to pursue and stop terrorists. The existing laws were written in the era of rotary telephones. This bill met with an overwhelming support in Congress because it upholds and respects civil liberties."

Analysis of the USAPA by the EFF*

"It seems clear that the vast majority of sections included have not been carefully studied by Congress, nor was sufficient time taken to debate it or hear testimony from experts. The civil liberties of ordinary Americans have taken a tremendous blow"

* Electronic Frontier Foundation

Patriot Act Successes

- Charges against 361 individuals
  - Guilty pleas or convictions for 191 people
  - Shoe-bomber Richard Reid
  - John Walker Lindh
- More than 500 people removed from United States
- Terrorist cells broken up in Buffalo, Seattle, Tampa, and Portland (“the Portland Seven”)

Patriot Act Failure

- March 11, 2004 bombings in Madrid Spain
- FBI makes Brandon Mayfield a suspect
  - Claims partial fingerprint match
  - Conducts electronic surveillance
  - Enters home without revealing search warrant
  - Copies documents and computer hard drives
- Spanish authorities match fingerprint with an Algerian
  - Judge orders Mayfield released
  - FBI apologizes
- Civil rights groups: Mayfield was targeted for his religious beliefs

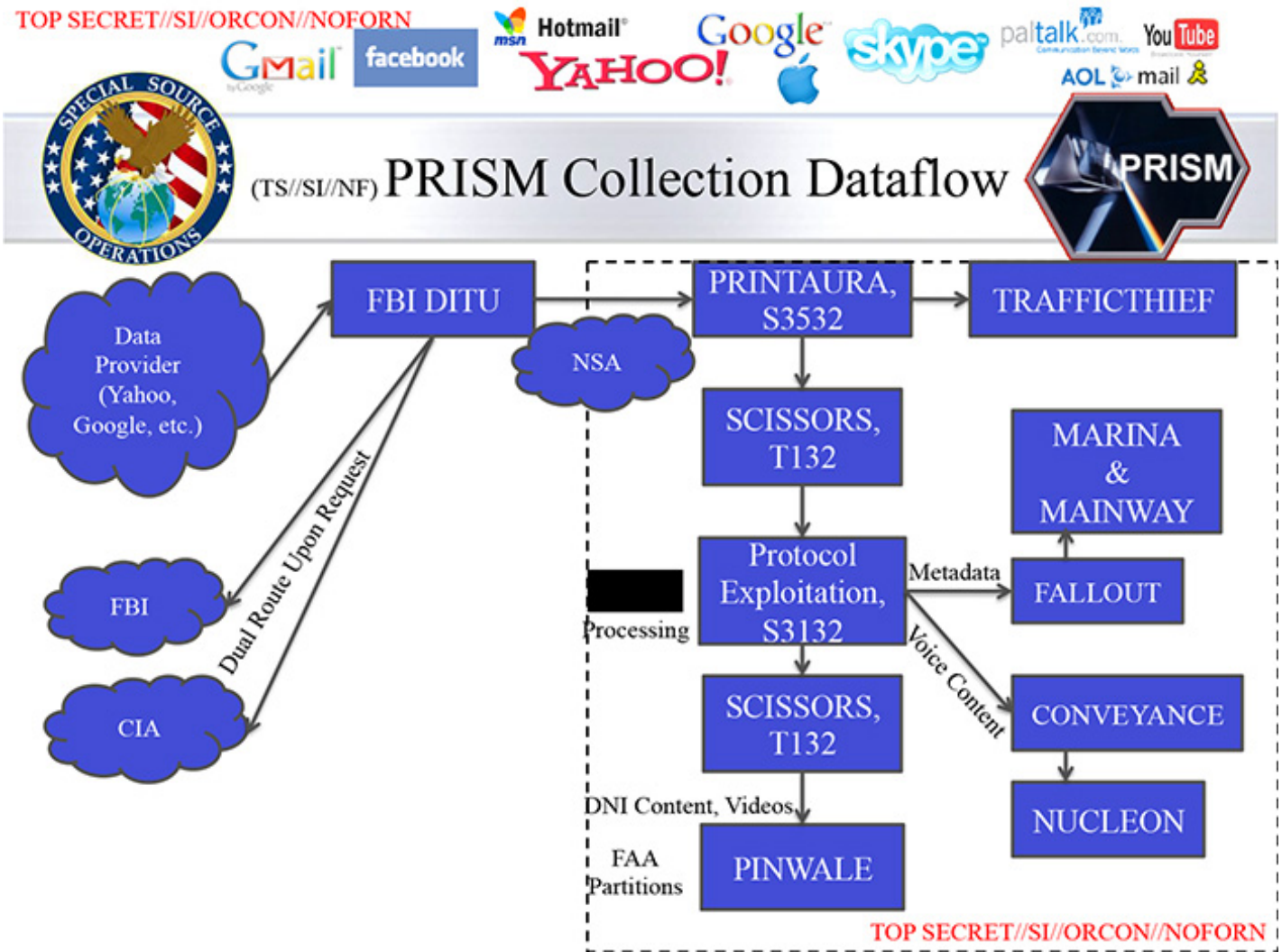
The PRISM Program

- PRISM is a code name for a program under which the United States National Security Agency (NSA) collects internet communications from various U.S. internet companies
- PRISM began in 2007 in the wake of the passage of the Protect America Act under the Bush Administration

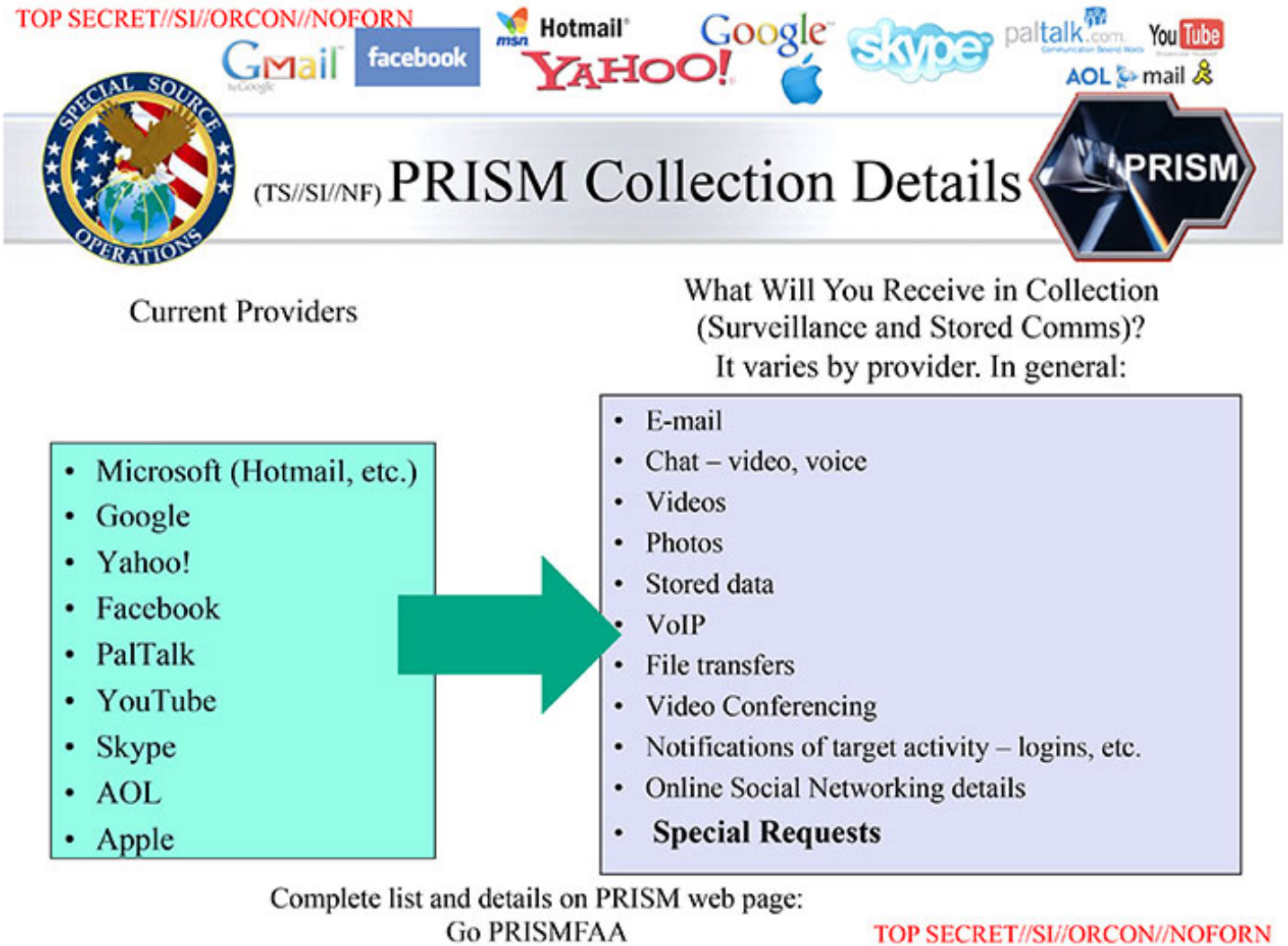
The PRISM Program

- Its existence was leaked six years later by NSA contractor Edward Snowden
- Snowden warned that the extent of mass data collection was far greater than the public knew and included what he characterized as "dangerous" and "criminal" activities.
- The disclosures were published by The Guardian and The Washington Post on June 6, 2013
- U.S. government officials have disputed some aspects of the Guardian and Washington Post stories and have defended the program by asserting it cannot be used on domestic targets without a warrant, that it has helped to prevent acts of terrorism, and that it receives independent oversight from the federal government's executive, judicial and legislative branches

The PRISM Program



The PRISM Program



Who Are the Stakeholders?

- Computer users in the public
- Internet Service Providers
- Libraries
- Law Enforcement
- Terrorists

Class Activity 1

Class Activity 2

Class Activity 2a: Ethical Question

- The Patriot Act allows for ISPs to “voluntarily” disclose information to law enforcement, how will the public view the ISP who “might” have had information which could have prevented a terrorist act?
  - Use an act utilitarian and social contract theory perspective.

Class Activity 2b: Ethical Question

- Is it ethical to allow ISPs to make the determination of whether or not there is an emergency involving immediate danger of death or serious physical injury to any person?
  - Use a Kantian and virtue ethics perspective.

Class Activity 2c: Ethical Question

- Is it ethical that the Patriot Act makes law enforcements job of apprehending criminals easier at the cost of affecting a greater number of innocents?