CS 4001: Computing, Society & Professionalism

Munmun De Choudhury | Assistant Professor | School of Interactive Computing

Week 8: The Patriot Act, Midterm Review

February 27, 2018

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

Who Are the Stakeholders?

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

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

NSA Access to Telephone Records

- Edward Snowden leaked documents to the *Guardian* newspaper
- *Guardian* revealed Foreign Intelligence Surveillance Court had ordered Verizon to provide NSA with all of its telephone metadata for 3-month period in 2013 (date, time, location, and length of call, but not contents of call)
- *Guardian* critique: NSA's mission now "focuses increasingly on domestic communications"
- Obama administration: Court orders for telephone records "are something that have been in place a number of years now"

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."

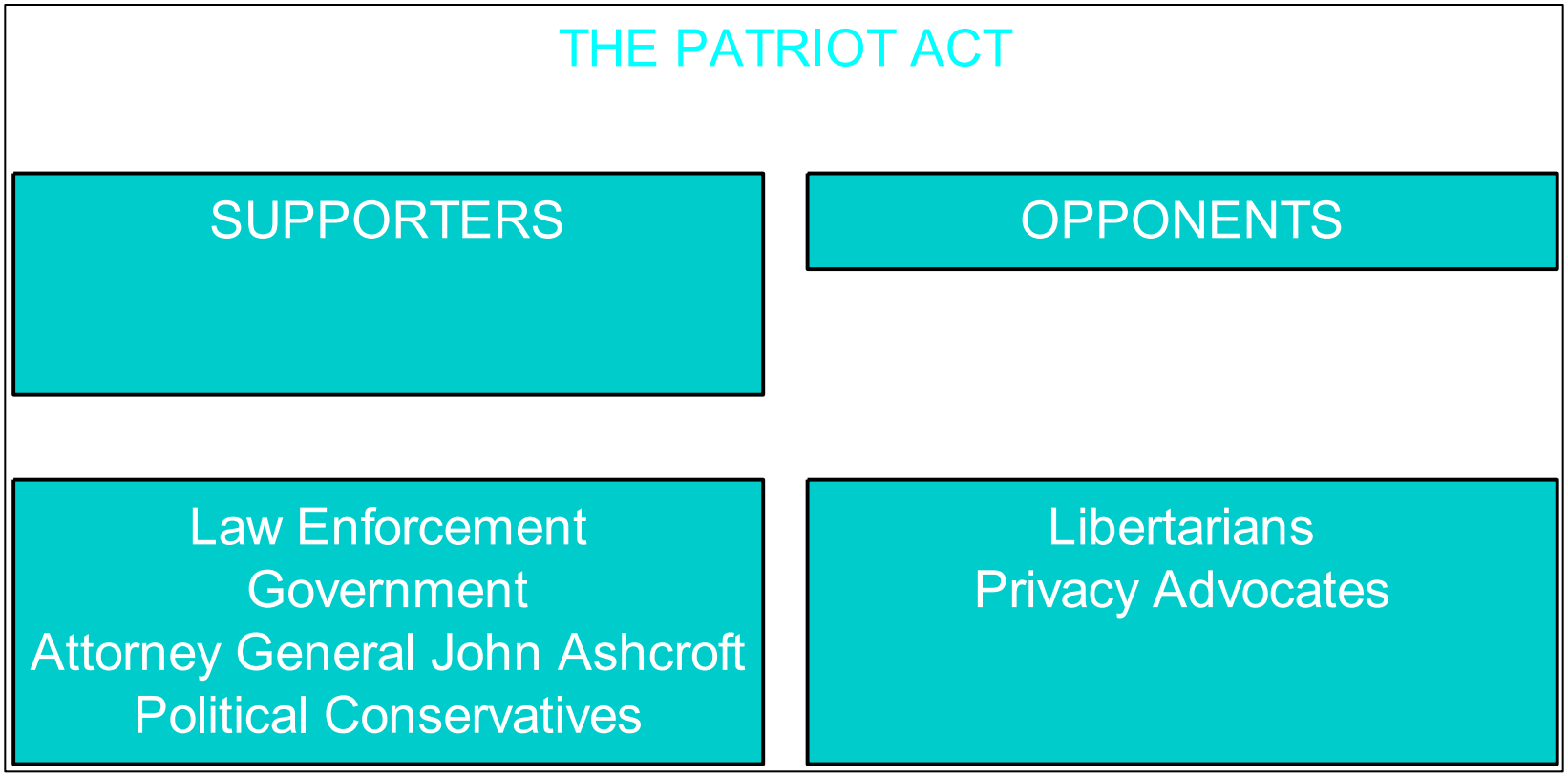
Analysis of the USAPA by the EFF*

"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

Class Activity 1

Advocates vs. Opponents



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

Case Study: Internet Service Providers

ISPs: Part of Corporate America

- They do not generally engage in criminal or terrorist activity
- There are large and small ISPs alike and the effects on both must be taken into account.
- The financial impacts on both must be taken into account

How does the USA Patriot Act affect ISPs?

- Allows ISPs to “voluntarily” disclose electronic communications
- In the event immediate danger or death or serious bodily injury to a person requires such disclosure.

Law Enforcement's POV

- Previous Law was inadequate
- No provisions allowing providers to disclose customer records or communications in emergencies
- Did not expressly permit a provider to voluntarily disclose "non-content" records to law enforcement for purposes of self protection
- Providers could disclose the content of communications for this reason

Civil Libertarians POV

- It allows ISPs to voluntarily handover all "non-content" information to law enforcement with no need for a court order or subpoena
- It expands the records that the government may seek with a simple subpoena (no court review required)

Pros

- ISPs may now authorize law enforcement to intercept a computer trespasser's wire or electronic communications
- No need for law enforcement to first obtain a court order before performing these surveillance activities
- Computer system operators can now obtain assistance from law enforcement when they are attacked by trespassing "hackers"
- The DOJ analogizes this new power to a homeowner calling the police

Cons

- CSPs may now voluntarily disclose information about users to law enforcement
- May now voluntarily disclose to the government user communications or customer records
- Financial burden on ISP / Additional Man power is uncertain

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?

Midterm Review

Ethics

Therac 25: What Happened

- Between June 1985 and January 1987, 6 known accidents involving massive overdoses, causing death & serious injury

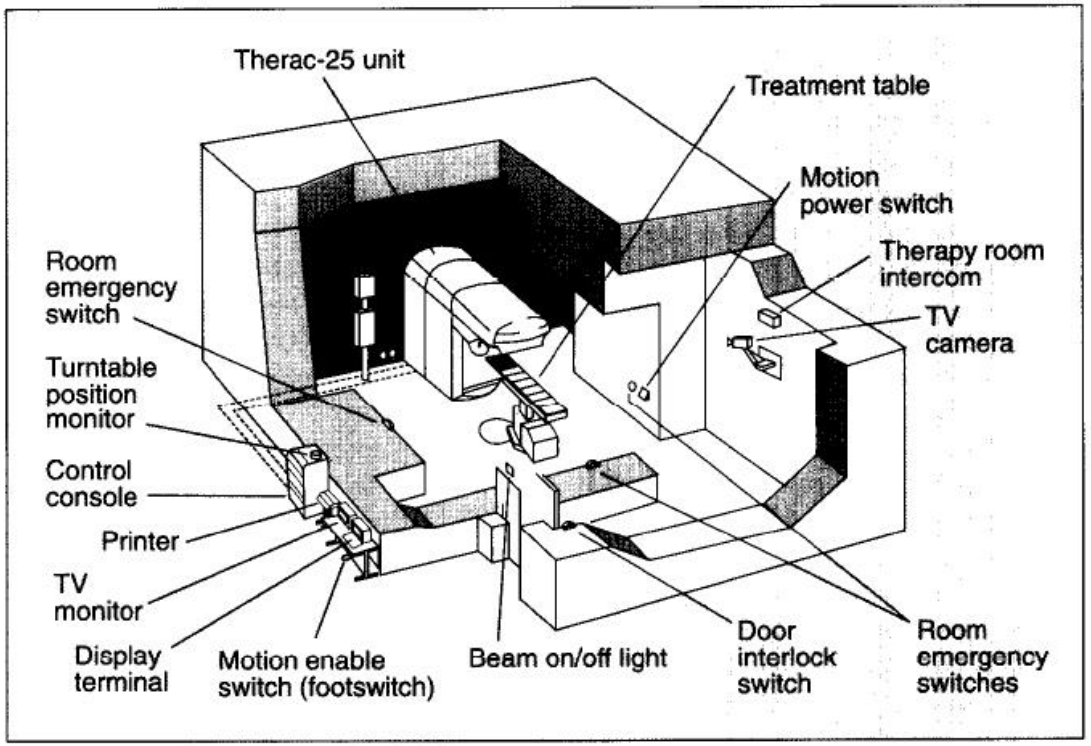


Figure 1. Typical Therac-25 facility.

Ethical Theories

- Formal study started with Socrates
- Ethical theories are frameworks for moral decision making
- We need ethical theories to examine moral problems behind an issue, reach conclusions, and defend those conclusions in front of a skeptical, yet open-minded audience
- Used to provide logical, persuasive justifications behind your reasoning in the case of an argument

Software Engineering Code of Ethics: 8 Key Principles:

- Product
- Public
- Judgment
- Client and Employer
- Management
- Profession
- Colleagues
- Self

Censorship and Internet

- Unlike traditional one to many broadcast media, the Internet supports many to many communications
- The Internet is dynamic – new devices are being connected each year
- The Internet is huge – human censors not practical
- The Internet is global – national governments have limited authority to restrict activities happening outside their borders
- It is hard to distinguish between different types of people e.g., children and adults on the Internet

Information Technology Erodes Privacy

- Information collection, exchange, combination, and distribution easier than ever means less privacy
- Scott McNealy (Sun Microsystems): “You have zero privacy anyway. Get over it.”
- This class: we will consider how we leave an “electronic trail” of information behind us and what others can do with this info

Solove's Taxonomy of Privacy

- **Information collection:** Activities that gather personal information
- **Information processing:** Activities that store, manipulate, and use personal information that has been collected
- **Information dissemination:** Activities that spread personal information
- **Invasion:** Activities that intrude upon a person's daily life, interrupt someone's solitude, or interfere with decision-making

Arguments

ARGUMENTATIVE ESSAY

The argumentative essay
is a genre of writing that requires you to:

1. investigate a topic;
2. collect, generate, and evaluate evidence; and
3. establish a position on the topic in a concise manner.

What is Evidence?

- “Evidence” I all the verifiable information a writer might use as a support for their argument, such as facts, observations, examples, cases, testimony, experimental findings, survey data, statistics, etc.

- Evidence is part of the “grounds” and “backing” of an argument in support of reasons and warrant respectively