Section II

Privacy and Legislation

Sanjay Goel & Christopher Brown,
School of Business, University at Albany, SUNY

Privacy and Legislation

Privacy Definition

What is privacy?

The Fourth Amendment:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Webster's:

The quality or state of being apart from company or observation; freedom from unauthorized intrusion.

Right to be reasonably left alone.

Privacy and Legislation

How Technology Infringes on Privacy

- The ability to share information by electronic means has affected personal privacy.
  - Data storage is becoming increasingly cheaper.
    - Large credit databases like Equifax and TransUnion
    - And it's not just your purchasing history…
  - Segregated sources of information can be integrated as physical location no longer matters.
    - Credit history, medical history, purchase history, etc
  - Computers are very good at conducting automated tasks.

Privacy and Legislation

Legislative History

- The Communications Act (1934)
- The Freedom of Information Act (1966)
- The Privacy Act (1974)
- The Electronic Communications Privacy Act (1986)
- The Communications Assistance for Law Enforcement Act (1994)
- Telecommunications Deregulation and Reform Act (1996)
- The children's Online Privacy Protection Act (1998)
- Gramm-Leach-Biley Act (1998)
- USA PATRIOT Act (2001)
- Health Insurance Portability and Accountability Act

Privacy and Legislation

HIPAA

- Title I:
  - Protects health care insurance when jobs are lost or changed
- Title II:
  - National standards for electronic transactions
  - Security safeguards
    - Administrative, Physical, Technical
  - Privacy safeguards
    - Individuals must have access to records
    - Individuals must be informed of data use
    - PHI cannot be used for marketing without consent
    - Entities must document privacy procedures
    - Entities must appoint a Privacy Officer

Health
Insurance
Portability and
Accountability
Act

Privacy and Legislation

USA PATRIOT Act

Uniting and
Strengthening
America by

Providing
Appropriate
Tools
Required to
Intercept and
Obstruct
Terrorism

- Passed in response to Sept. 11th terrorist attacks.
- Gives "federal officials greater authority to track and intercept communications… for law enforcement and foreign intelligence"
  - telephone lines
  - emails in 3rd party storage
  - pen registers and trace-and-tap device use
- New crimes, penalties, and procedures against domestic and foreign terrorists

Source: http://www.fas.org/irp/crs/RS21203.pdf

Privacy and Government

Privacy and Government
Dilemma

- There has always been a concern about the government intruding into the privacy of citizens
  - There have been 10 major legislations affecting privacy
- The government has legitimate needs for monitoring people
  - Tracking illegal activities
  - Child and spousal abuse
  - Terrorism
  - Espionage
  - Demographic Studies

- What is the balance between citizen privacy & citizen security?

Privacy and Government

NSA Phone-tapping Program

- Warrant-less phone-taps on individuals in the U.S. calling persons or suspected terrorists abroad.
- Authority granted to NSA to eavesdrop on suspicious emails.
- ACLU has filed a lawsuit claiming the program violates both the Constitution and a Federal law claiming that a court order is generally necessary to eavesdrop.
- Should the NSA conduct warrant-less surveillance on those suspected of communicating with terrorists?

Privacy and Government

Long History of Government Surveillance

- ***Revolutionary War*** – General Washington intercepted letters
- ***Civil War*** – President Lincoln wiretapped telegraphs
- ***World War I*** – President Wilson intercepted every type of communication leaving the country
- ***World War II*** – President Roosevelt authorized listening devices; military authorized to intercept and review all telecommunications passing between the United States and foreign countries

Privacy and Government

ECHELON Program

- NSA (National Security Agency) global spy system developed in the 1960's to assist in Cold War
- Made up of a network of "listening posts"
- Ability to intercept electronic communications, e.g.
  - Email
  - Telephone conversations
  - Fax
  - Fiber-Optic Communications
  - Microwave Transmissions
  - Satellite Communications
- Some estimate ECHELON intercepts 3 billion communications daily

- "If you made a phone call today or sent an e-mail to a friend, there's a good chance what you said or wrote was captured and screened by the country's largest intelligence agency." (Steve Kroft, CBS' 60 Minutes, February 27, 2000)

Privacy and Government

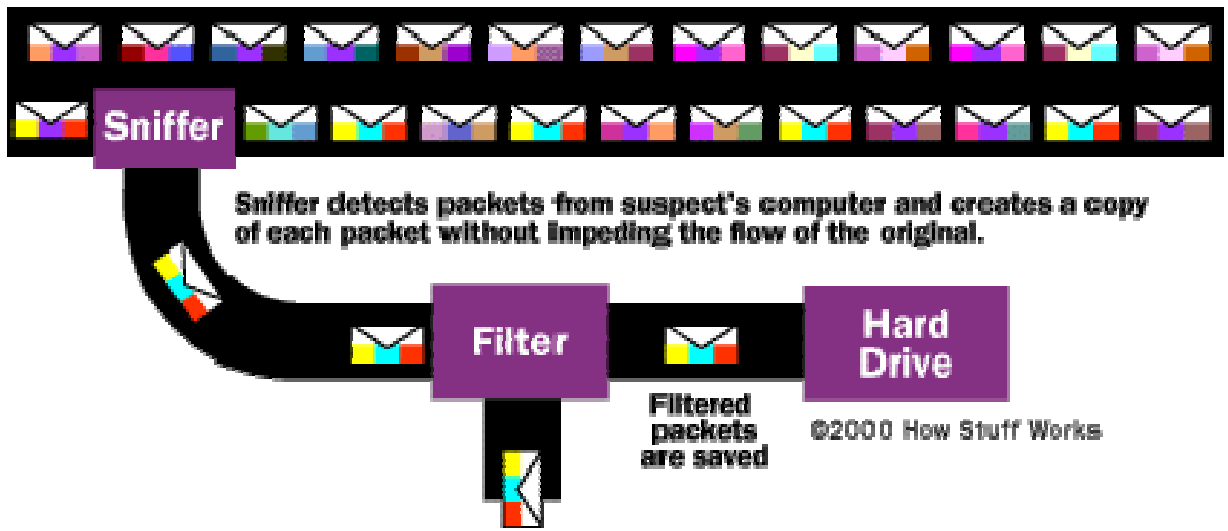
Carnivore

- Carnivore was a "content wiretap for email"
  - "trap-and-trace" and "pen-register" much more restrictive
- In Content wiretap mode, FBI could eavesdrop on Internet communication
  - capture all e-mail messages to and from a specific user's account

Privacy and Government

Carnivore (Technology)

- The actual Carnivore box was installed at an ISP
  - Lacks a monitor and a keyboard
- Essentially Carnivore was a packet sniffer.
  - Intercepted the packets and made copies of selected packets for processing
- Carnivore was a passive wiretap and did not interfere with communication.



Privacy in the Workplace

It's not government that is emerging as the clearest embodiment of Big Brother — the all-seeing, all-knowing entity in Orwell's novel "1984" — but Corporate America.

-- AP. (September 1, 2003). Big Brother: It's not government, but corporate America doing the spying. USA Today.

Privacy in the Workplace

Employee Profiling

- Computer profiling and matching personal data to that profile
  - Mistakes can be a major problem

- If corporations can get the health records of applicants can they discriminate?

Privacy in the Workplace

Employee Monitoring

- Monitors individuals
- Is done continuously. May be seen as violating workers' privacy & personal freedom
- Workers may not know that they are being monitored or how the information is being used
- May increase workers' stress level
- May rob workers of the dignity of their work and decrease morale

Privacy in the Workplace

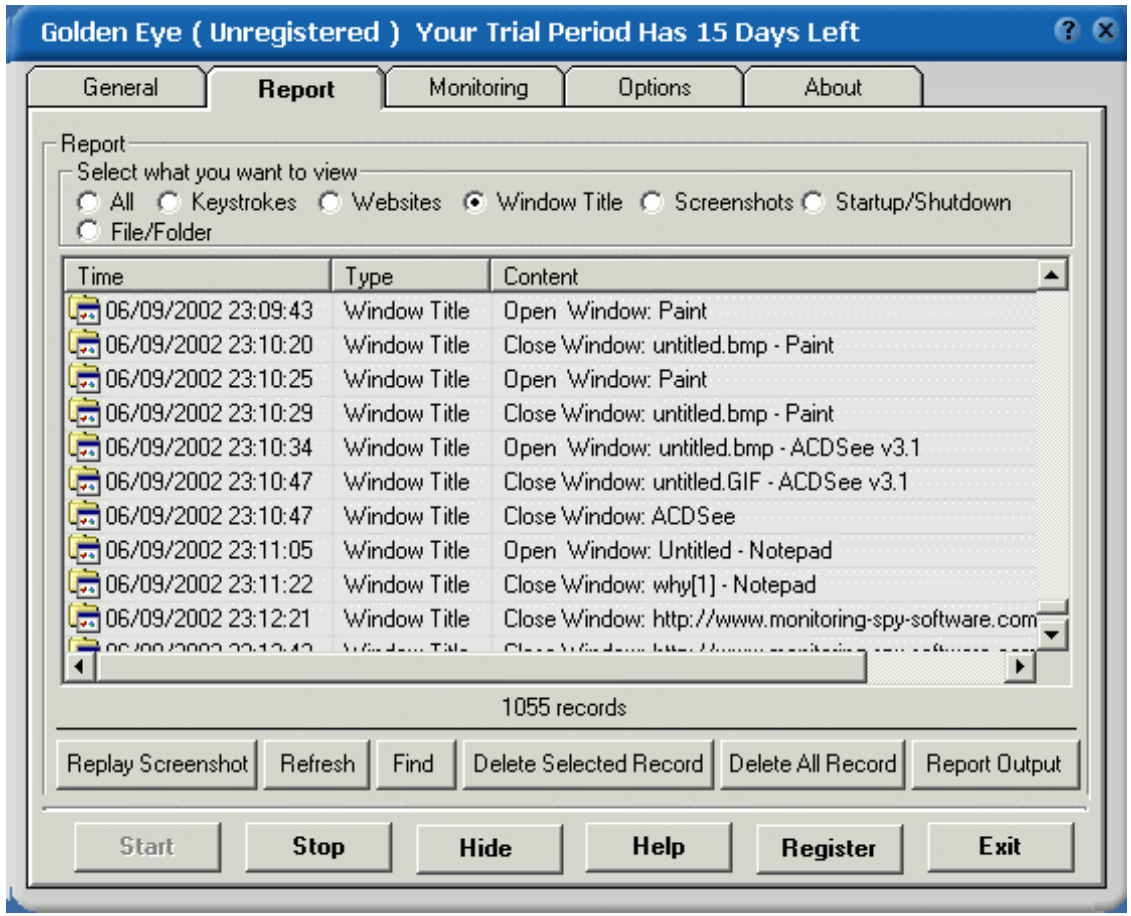
Electronic Monitoring

- Examples
  - Email Monitoring (emails sent and received)
  - Instant Messaging (custom-made for employers)
  - Entrance Systems (radio frequency ID cards, can be used to pinpoint location)
  - Computer Logins (when someone logs in)
  - Logs (Errors with login, connections, etc.)
  - Keystroke Logging (All applications, actions, & keys pressed)
  - Packet-sniffing (Internet traffic)

Privacy in the Workplace

Keystroke Loggers

- Monitor and keeps track of all actions made on the computer.

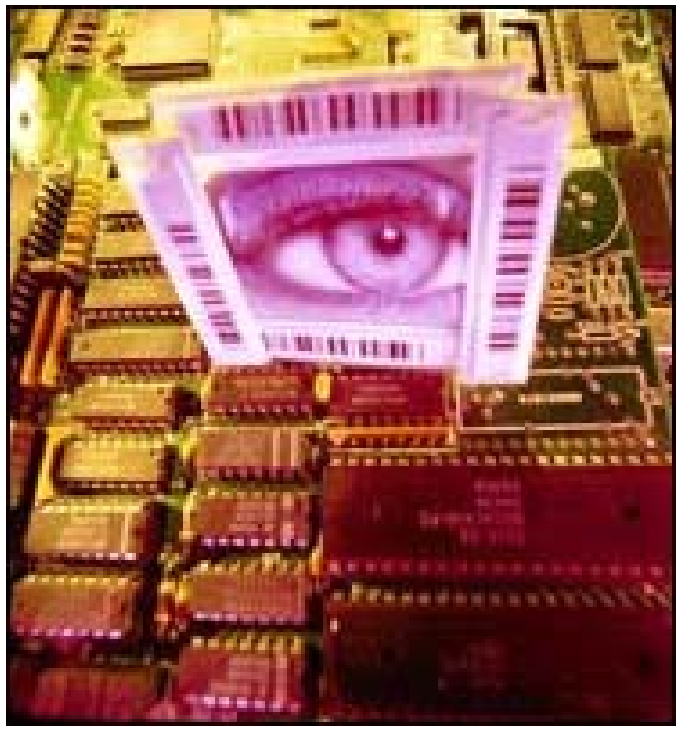


Privacy in the Workplace

Reasons for Monitoring

In a 2005 survey about electronic monitoring…

- Employees believe:
  - productivity
  - control
  - distrust
- Employers say:
  - viruses
  - hackers
  - corporate secrets



Source: Claburn, T. (January 20, 2005). Survey Suggests Employees Doubt Workplace-Monitoring Motives. *Information Week*.

Privacy in the Workplace

9/11 Effects

- In a February 2002 Harris Poll, it was found that:
  - 81% of employed adults said they were willing to have ID cards issued by their employers, with photos, fingerprints (or some other biometric identifier), with 44% claiming to be very willing and 7% "not at all willing."
  - 36% said their employers have made identification procedures more stringent for people entering their workplaces.
  - 26% said that stricter procedures for accessing their employers' computer systems are now in place.

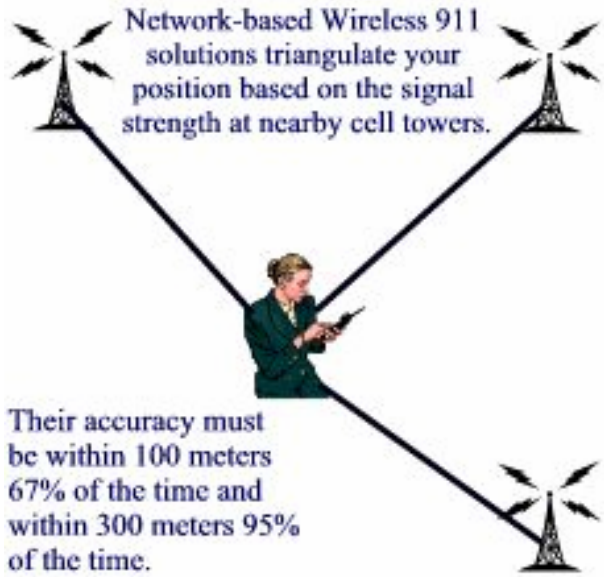
Section V

Other Privacy Issues

Other Privacy Issues

Examples

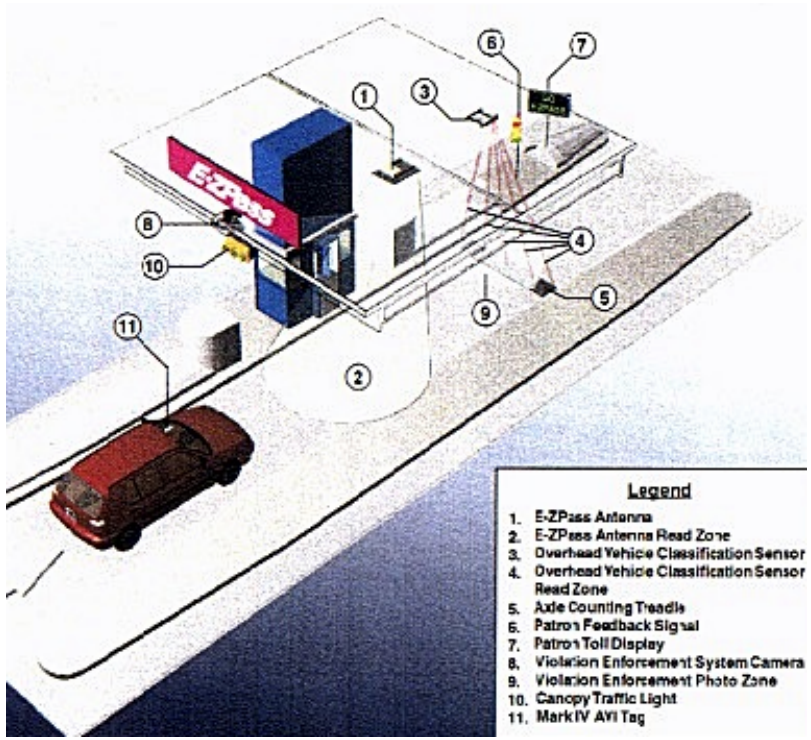
- Accessing private e-mail and computer records & sharing information about individuals gained from their visits to websites and newsgroups
- Always knowing where a person is via mobile and paging services
- Using customer information obtained from many sources to market additional business services
- Collecting personal information to build individual customer profiles



Other Privacy Issues

EZPass

- EZPass is a transponder that emits a radio signal which is read by a toll booth with the appropriate equipment.
- Convenience
  - Don't have to stop to pay tolls
  - No change
  - No need to have person to collect tolls
- Effects on privacy
  - Signal emitted can be traced from one EZPass station to the other. Potentially could be tracked using this signal to find out how fast you drove from Albany to New York City or to estimate locations.



Source: http://www.itsdocs.fhwa.dot.gov/jpodocs/repts_te/@6L01!.pdf

Other Privacy Issues

RFIDs in Society

- **Passports** – includes data contained on page of the passport, including name, date and place of birth, and a digitized version of the passport photo. Will not be encrypted, however, will have a read range of inches.
- **Currency** – Proposed to be put into European Union currency, suggested that this has been implemented in US $20 bills.
- **Pets** – implanted in the necks of pets to track them and find them if they get lost.
- **Children** – RFIDs are placed in clothing, name tags, and book bags to keep track of school children in Japan as well as in Denmark's Legoland.

Sources: http://www.wired.com/news/privacy/0,1848,66686,00.html?tw=wn_tophead_1 http://networks.silicon.com/lans/0,39024663,39122042,00.htm

Other Privacy Issues

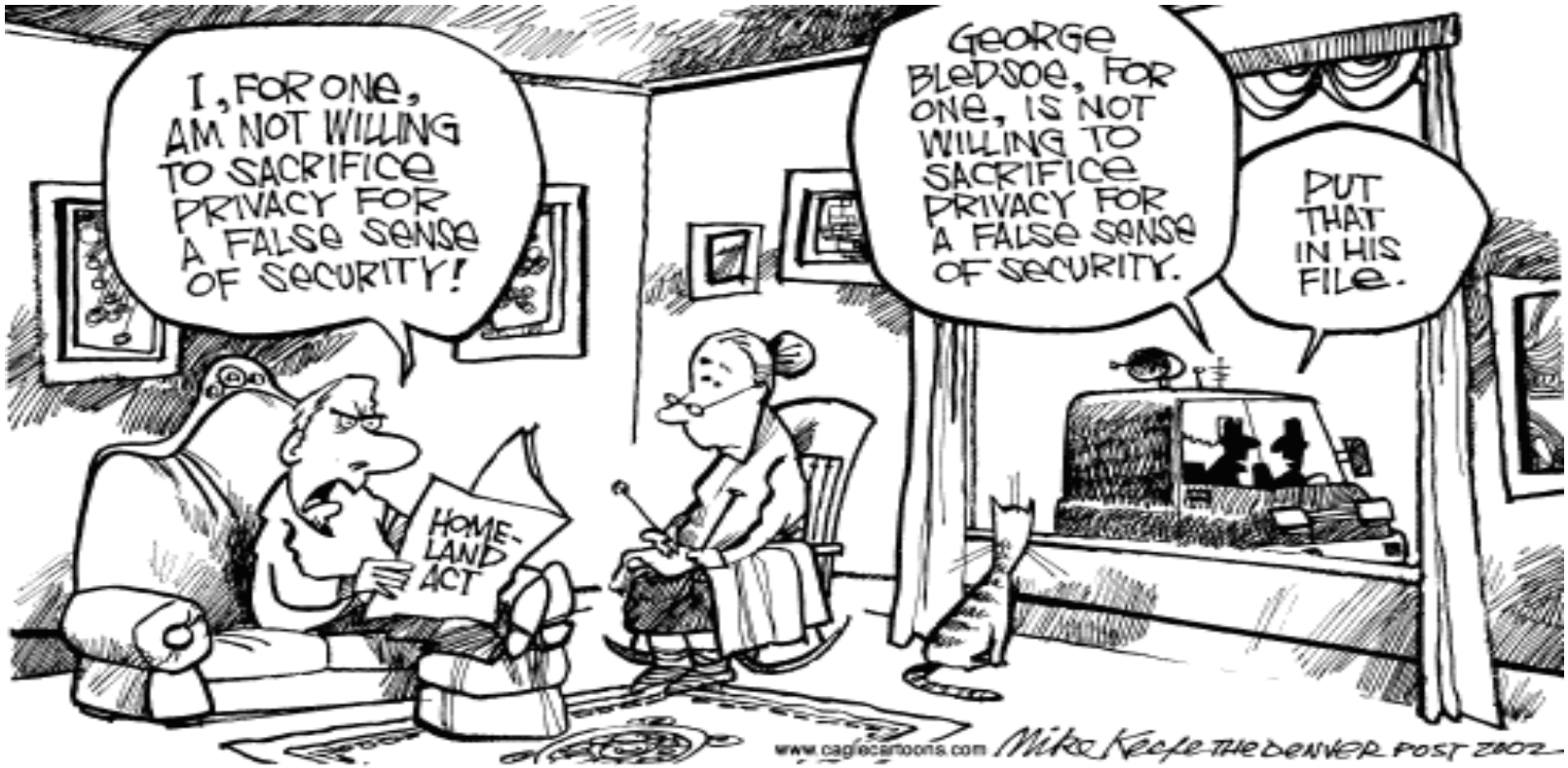
RFID

9/30/04 Wired News – Watchdogs push for RFID Laws

"RFID is too powerful a technology and Wal-Mart and its suppliers are too cozy with the U.S. Department of Homeland Security for the companies to be trusted with the data gathered from radio tags on consumer goods, say a civil rights lawyer and a privacy law expert".
These tags can be used to monitor products from the shelves of a store to checkout as well as allow for constant updating of inventory. However, stores want to keep these RFIDs active even when the products leave the store to associate the products bought to the customers who bought them. This can be used for anything from creating customer profiles for better marketing or for investigating suspected terrorists. "The surveillance potential for RFID is huge".

Source: http://www.wired.com/news/digiwood/0,1412,65162,00.html?tw=wn_tophead_13

Conclusion



- Technology is an enabler
- Privacy can be violated by many different entities