CS305 Topic – Privacy

- Concept Evolution
- Rights to Privacy
- Privacy and Technologies
- US Privacy Laws

Sources: Baase: A Gift of Fire *and* Quinn: Ethics for the Information Age

Privacy

The original privacy concept is *physical privacy* — Freedom from intrusion or "to be let alone".

- Protecting privacy means preventing intruders from entering private properties without authorization.
- 4th Amendment to the Constitution:

> 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.

Privacy Concept Evolution

With the technology advances, comes the need to extend the privacy concept:

- Freedom from surveillance (from being followed, tracked, watched …)

  The issue first came up when telephone was invented in late 19th century – wiretapping violates peoples' privacy, even though their physical private properties are not compromised.

Informational Privacy

- Control of Info About Oneself — Having full control over what information about oneself to give and whom to give to.
  - Name and address, DOB, Physical info
  - Family info, Job info
  - Travel info, Shopping habits
  - …

Rights to Privacy

How much privacy are we entitled to?

- Privacy is a *natural right*. (Warren and Brandeis [1890])

Question:

Can we afford absolute privacy right to everyone?

Harms of Too Much Privacy:

- Harder for others to really know a person
- Easier for some people to plan and carry out illegal or immoral activities
- Conflicting with other people's rights

Rights to Privacy (cont.)

How much privacy are we entitled to?

- Privacy is a *prudential right*. (Benn and Reiman [1984])
  - *Granting privacy rights benefits the society:*
    - Allow people to be unique individuals
    - Foster creativity, spirituality, relationships, etc.
  - *However, privacy rights must be balanced with other rights*

How to Balance?

- Privacy *vs.* Safety and Security
  - E.g. government surveillance
- Privacy *vs.* Desire for Free Expression
  - E.g. news articles
- Privacy *vs.* Convenience
  - E.g. telephone number listing
- Privacy *vs.* Need for Credentials
  - E.g. loan applications

Privacy and Technology

RFID chips!

Privacy and Technology

Technologies have made information collection, storing, and access much easier.

- Personal info easily become public
- Databases everywhere
- Data mining becoming more powerful
- Surveillance technology becoming more sophisticated

On the positive side,

- Encryption techniques

Challenges

- Footprints and fingerprints everywhere
- Big brother is watching
  - Government surveillance and data mining
- Big sister is watching
  - Commercial companies have lots of information about you
- Little brother is watching
  - Public documents become very public
  - Everyone can be a detective

Loss of Privacy

- We are leaving an “electronic trail”
- History of government abuses
- Identity theft
- Loss of privacy = loss of self ???
  - “1984”, by George Orwell
- Privacy for spiritual growth, creativity

Digital Footprints

- Bank and credit card activities
- Web surfing records
- GPS and cellphones
- Black boxes in cars
- Smart parking garages
- Meta data in documents
- Tracing paper

Public Information

Personal info can easily become public:

- Personal info in blogs and online profiles
- Pictures of ourselves and our families
- Consumer product registrations

Question:

- Young people seem to put less value on privacy than previous generations. Is privacy old-fashioned? Or they don't understand the risks?

Telemarketing

- The Do-Not-Call Registry
  - Established by the FTC
    - Exceptions: Charities, Political Orgs, Surveys
  - Public loves it
  - Violations are occuring

Modern Technology

- Does prosperity contribute to isolation?
  - Automobile
  - Television / Movies / DVDs
  - Telephone
  - Computer / email / voice mail
  - Single-family homes / Big cities
    - We live amongst strangers!

Public Records

Many records are available to the general public:

- Property records, bankruptcy records
- Salaries of government employees
- Arrest records, etc.

Access vs. Privacy:

- How should we control access to sensitive public records?
- Recent debate: Firearm ownership records

Digital Cameras

Taking pictures on public property. Does it violate privacy?

- Google Street View
  - Captures whatever camera sees at the time
- Digital Cameras in general
  - Panavision 300x optical zoom (see YouTube video for effects)

Laws:

- On public property, “if you can see it, you can shoot it” (additional restrictions on zooming in on people)
- You may not be able to publish what you shot

Video Surveillance

- Tampa, FL police scanned the faces of all 100,000 attendants of the 2001 Super Bowl.
  - A computer system searched files of criminals for matches, and returned results in seconds (none was found)
  - People were not told that their faces were being scanned
- The UK has one surveillance camera for every dozen citizen. In London, an average person is photographed hundreds of times a day by surveillance cameras.

Other Technologies

- Cell phones: Location Tracking
- RFID tags (radio freq. ID)
  - Put into products for inventory control
    - They are never deactivated
  - In passports
    - Terrorists scan cafes/targets for foreigners!
  - Implanted in pets… or people.
- Cookies – to track web usage

Government Databases

The government maintains many databases. Among them:

Census Records, IRS Records, FBI NCIC Database

Questions:

- Who can create and keep databases of personal information?
- Who has right to access these databases?

Example Case:

- Nixon had the IRS audit the tax returns of individuals on an “enemies list.” (It was legal.)

Kinds of Information

- Public Records (Governemnt records)
  - Marriage certificates, arrest records, legal deeds, etc.
- Public Information
  - Info available from companies, Internet, …
- Personal Information
  - What's left? Your secrets?

Code of Fair Information Practices

Proposed by an US study group in the early 70s. Adopted later by many governments, including US:

- No secret databases
- People should have access to personal information in databases
- Organizations cannot change how information is used without consent
- People should be able to correct or amend records
- Database owners, users responsible for reliability of data and preventing misuse

Privacy Act of 1974

Codification of the proposed principles.

- Existence of personal-info databases must be disclosed.
- Everyone has a right to know what info about him/her-self is in the databases.
- Consent is required if personal-info is targeted for non-intended uses.

Loopholes of the Privacy Act

Only applies to government databases.

- Far more info is held in private databases

Only covers records indexed by a personal ID.

- One has no right to access his/her info if record is not keyed to his/her ID

No one is in charge of enforcing the law.

- Many exceptions have been given

Allows records to be shared among agencies as long as they are for "routine use".

- Each agency defines "routine use" for itself

Other US Privacy Laws

Fair Credit Reporting Act [1970]

- Promotes accuracy and privacy
- The Main Credit Bureaus / Credit Scores
  - Equifax, Experian, TransUnion
  - You can request your information
- Negative information kept only 7 years
  - Criminal convictions forever
  - Bankruptcies for 10 years (?)

Other US Privacy Laws

Family Education Rights and Privacy Act [1974]

- Rights to access/change/release educational records are given to student (18yrs or older) or his/her parents

Video Privacy Protection Act [1988]

- Videotape service providers cannot disclose rental records without consumer's written consent

Other Privacy Laws (cont.)

Health Insur. Portability and Accountability Act [1996]

- Limits how doctors, hospitals, pharmacies, and insurance companies can use medical information

Financial Services Modernization Act [1999]

- Privacy policies must be disclosed to customers
- Notices must provide an opt-out clause
- Must develop procedures to protect customers' info

Children's Online Privacy Protection Act [2000]

- Reduces amount of public information gathered from children – must be 12 or older

Data Mining

- Info about customers is a valuable commodity
- Searching for patterns or relationships in one or more databases
- Secondary use

Examples:

- Marketplace: Household
- IRS audits
- Total Information Awareness

Total Information Awareness

Proposed by DARPA in 2002.

- Combine *all* financial, medical, travel, communication, and other records into TIA databases
- Try to capture "information signatures" and look for terrorist-like patterns of activity

Faced Major Objections:

- ACM wrote an open letter of objection to the program.
- Congress later limited the scope; suspended funding
- DARPA renamed the program to Terrorist Information Awareness.

The OneDOJ Database

Dept of Justice, FBI, Drug Enforcement,
Bureau of Alcohol,Tobacco&Firearms,
Bureau of Prisons

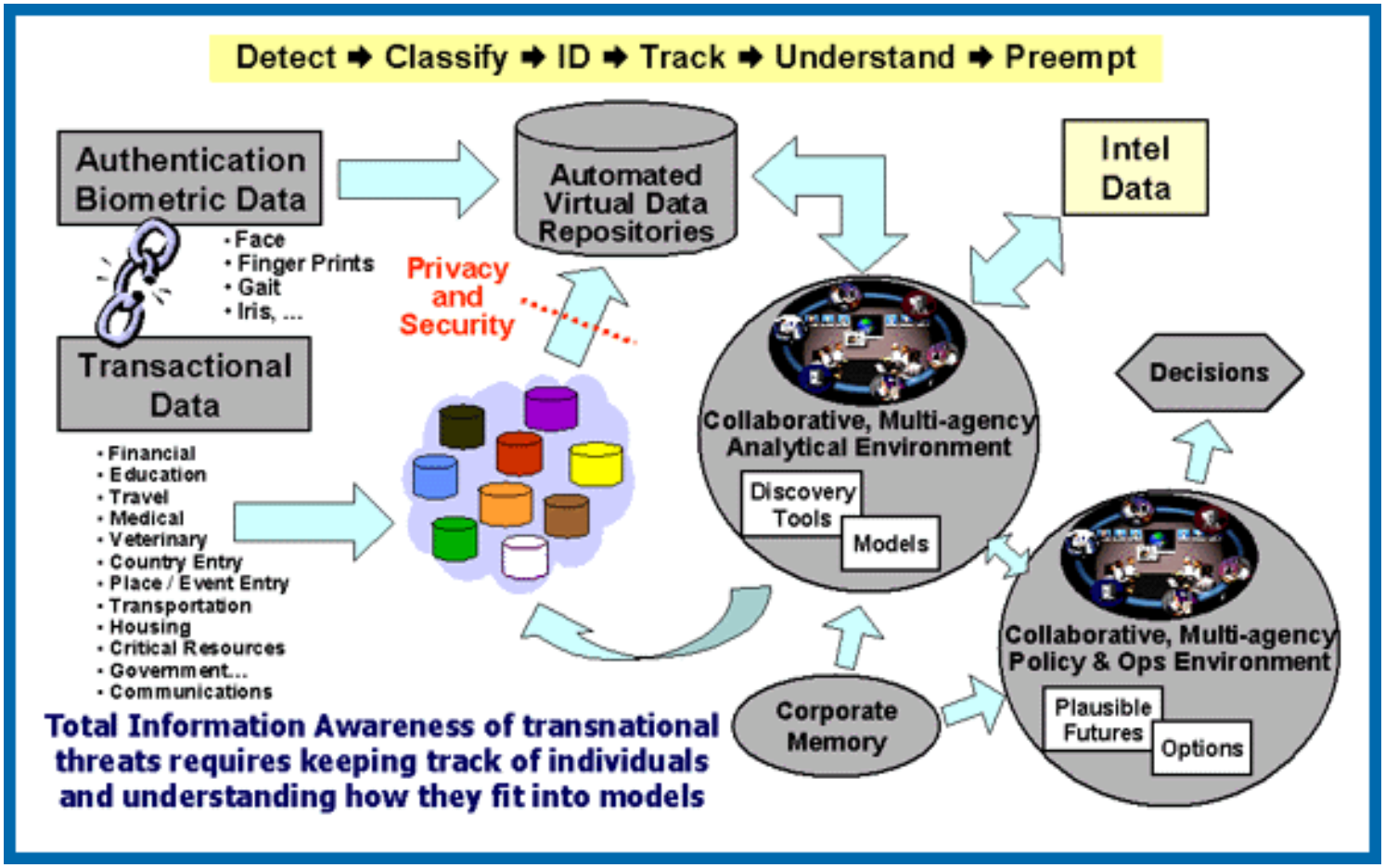
Stores incident reports, interrogation summaries, etc.

Raw Police Files

…can never be verified or corrected.

May contain info about people who are not criminals.

TIA System Diagram



Identity Theft

Misuse of another person's identity to take actions permitted the owner.

- Gaining Access to Information through

  mailboxes, lost or stolen wallets, dumpster diving, shoulder surfing, phishing, …
- Credit card fraud #1 type of identity theft
- Ease of opening accounts contributes to problem
- 10 million victims in 2004 alone, average loss: $5,000

National ID Cards?

Arguments For:

- Current ID cards are second-rate
- Would reduce illegal entry to U.S.
- Would reduce crime
- Other democratic countries have national ID cards

Arguments Against:

- No card positively guarantees identification
- No biometric-based system is 100% accurate
- No evidence it will reduce crime
- Makes government data mining simpler

The REAL ID Act (2005)

Significantly changes driver's licenses in the United States. New licenses

- Issued by end of 2008
- Required to open bank account, fly on commercial airplane, or receive government service
- Requires applicants to supply 4 different Ids
- Will probably contain a biometric identifier
- Must contain data in machine-readable form

Government Wiretapping

- Omstead v. United States [*1928*]
  - Supreme Court ruled wiretapping OK
  - Public opposed
- Federal Comm. Act [*1934*]
  - Made wiretapping illegal with no exceptions

… yet, *FBI continues secret wiretapping* …

- Katz v. United States [*1967*]
  - *Case:* public phone, FBI placed a bug *outside* of the phone booth
  - *Court Ruling:* bugs not OK

Wiretapping (cont.)

US Legislation Authorizing Wiretapping:

- *Omnibus Crime Control and Safe Streets Act [1968]*
  - With court order, up to 30 days
- *Electronic Comm. Privacy Act [1986]*
  - Extended wiretapping to electric communications
- *Comm. Assistance for Law Enforcement Act [1994]*
  - Requires digital telephony equipments be modified to allow wiretapping and tracing

USA PATRIOT Act of 2001

Provisions:

- Greater authority to monitor communications
- Greater powers to regulate banks
- Greater border controls
- New crimes and penalties for terrorist activity

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 linked to 911 attacks removed from US
- Terrorist cells broken up in Buffalo, Seattle, Tampa, and Portland (“the Portland Seven”)

PATRIOT Act Failures

- 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

Criticism of the PATRIOT Act

"The Act undermines Forth Amendment rights".

- Pen registers on Web browsers
- Roving surveillance
  - Can remotely turn on your cell phone and turn it into a live voice recorder.
- Searches and seizures without warrants
- Warrants issued without need for showing probable cause

Encryption

- Public key cryptography
  - No need to communicate keys
  - Strong encryption: virtually impossible to figure out private key, given public key
  - U.S. export restrictions (removed in 2000)
- Pretty Good Privacy
  - Phil Zimmerman created PGP (a public key encryption program); made it available on Internet
  - U.S. government threatened legal action

Electronic Money

An application of public-key encryption.

- When issuing electronic money, a bank signs it with its private key. Customers and merchants can use the bank's public key to verify the authenticity.
- Bank customers can use their private key to withdraw funds. The bank uses the customer's public key to verify the identity of the customer.

Digital Cash – anonymous electric money

- Relies upon blind signature protocol
- Cannot trace back to the original buyer

"You know, you can do this just as easily online."

Discussion Questions

- Compared to people who lived 50 or 100 years ago, do you think we have more or less privacy today?

- Facebook, introduced “news feeds” and “mini-feeds” in 2006. Mini-feeds sent recent changes in a member’s profile to all the member’s friends. What’s your opinion on this?

Discussion Questions

- Are you generally comfortable with disclosing personal info in exchange for free stuff?

- *Debate:* "Opt-in" vs. "Opt-out" policies in governing secondary use of information collected by merchants.