



Computers and Society

Privacy

Chris Brooks

Department of Computer Science

University of San Francisco



Privacy

- One of the big concerns that people often have with respect to information technology is protection of privacy.
- But what does “privacy” mean?

Types of Privacy

- We can divide questions about privacy into three categories:
 - Freedom from intrusion - being left alone.
 - Control of your personal information
 - Freedom from surveillance
- None of these concerns are absolute - they may need to be balanced against other concerns, such as public safety.

Analog privacy in the US

- In terms of pre-digital privacy, Americans have fairly extensive rights
 - Property may not typically be seized by the state
 - Fourth Amendment rights
 - In general, you can assume a large degree of privacy in your home.
 - In public, this is not the case.
- How to reconcile analog approaches to privacy with digital technology?

Your personal information

- One consequence of databases, online shopping, and e-government is that many individuals, companies, and organizations have access to information about you.
- There may be very good uses for this information.
- What organizations are you aware of that have personal info about you? How do they use it?

Some examples

- Supermarket club cards
- ISPs
- Cookies, click-through tracking
- Amazon - tracking purchases
- Universities
- Credit cards
- Online retailers
- State and Federal government

Advantages of collecting personal info

- Why might you be willing to give these groups your information?

Advantages of collecting personal info

- Why might you be willing to give these groups your information?
 - Targeted deals
 - Notification about new products
 - Ease of use
 - Necessary for transaction

Concerns with collecting personal info

- Why might you worry about giving your personal information to a third party?

Concerns with collecting personal info

- Why might you worry about giving your personal information to a third party?
 - Spam, telemarketing
 - Information sold to third parties
 - Information processed by untrustworthy parties
 - Information inadvertently revealed
 - Identity theft
 - Government retribution

Google

- As an example, you can use Google to look up a person's name and address, given their phone number.
- You can then use Google Maps to find their house.
- What are some valid uses of this technology?
- What are some potential misuses?
- How might Google balance advantages against potential privacy concerns?

Shopping habits

- Many supermarkets provide discount cards or club cards.
- Why do they do this?
- What information would you be willing to provide to a retailer? What guarantees would you want?
 - Personal info?
 - Anonymized buying habits?
- What would you want in return?
 - Special bargains?
 - Targeted ads?
 - Members-only events?

Case Study

- A business maintains a database containing the names of people convicted of shoplifting. It distributes this database to businesses that subscribe.
 - Is this an invasion of privacy?
 - What are arguments for and against?

Case Study

- A business maintains a database containing the names of landlords who are accused of providing adequate services. It distributes this database to San Francisco renters.
 - Is this an invasion of privacy?
 - What are arguments for and against?

Discussion

- Recent Federal law called the “enhanced 911 mandate” requires cell phone providers to be able to track the locations of active cell phone users to within 100 meters.
- Group 1: First responders (firemen, police)
- Group 2: cell phone providers
- Group 3: privacy advocates
- What are the advantages of this? What are the disadvantages? What could be done to address these concerns?

Information Leakage

- A common problem with electronic storage of personal information is information leakage.
- You may trust the entity that you provided your information to, but they might pass that information on to a third party.
- Examples:
 - Credit card companies
 - Retailers
 - USF
 - AOL search data

Surveillance

- A big concern recently has been the ability of third parties (particularly the government) to monitor private conversations.
- There is a delicate balance between personal privacy and national security.

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.”
- In a nutshell, your house and personal property is private, and cannot be searched without a warrant, which cannot be issued without probable cause.
- Question: where does one’s ‘person’ begin and end?

Wiretapping terminology

- Wiretapping generally refers to eavesdropping on a telephone conversation.
- A search warrant is required to get a wiretap, which is usually associated with a particular phone.
- Agencies may also get a *pen register*, which is a device that displays the incoming and outgoing phone numbers, but not the content of the conversation.
 - Standard is lower, since less information is revealed.
 - Cell phone companies also keep this information.
 - It can often be purchased from third parties without any stated reason.

Phone conversations

- A court order is needed to legally intercept the contents of a phone conversation.
 - Limited time period.
 - Tied to a particular number and person
 - A human must listen and decide whether a phone call is pertinent or not.

Logging Activity

- Law enforcement officials can also get what's called a *pen register*, which logs all outgoing calls.
 - Lower standards, since content is not being captured.
- Law enforcement officials can also obtain a *trap-and-trace*, which logs incoming calls.
- Again, burden of proof is lower since no content is being captured.

Email

- How does this apply to email?
- Court order needed to intercept or read stored email.
- Headers can be captured with the same authority as a pen register.
 - Question: Can headers contain more information than a phone number does?

Carnivore

- Carnivore is a tool developed by the FBI to monitor a suspect's Internet traffic.
- It serves as a “packet sniffer”; can be programmed to capture all types of traffic allowed by a court order.
 - For example, email, but not web traffic
 - Just email addresses, but not contents
- Issue - in order to determine what to keep, all content must be analyzed and other data discarded.
- Potential abuses?

Carnivore

- A digression -hypothetically speaking, how might one circumvent a system like Carnivore?

Carnivore

- A digression -hypothetically speaking, how might one circumvent a system like Carnivore?
- Encrypt data, either with RSA/PGP or by using SSL.
- Use out-of-band communications. For example, send email via port 80.
- Embed data in plain sight (steganography)

FISA

- Currently, there is a controversy involving the NSA monitoring phone conversations of US citizens without warrants.
- In order to monitor the conversations or communications of US citizens or of legal residents within the US, a court order is required.
- Post-Watergate, Congress realized that it was important to provide mechanisms that provided oversight of domestic surveillance while also allowing the secrecy needed for national security.
- Court orders are public - obtaining one might alert foreign operatives that they are being monitored.

FISA

- The Foreign Intelligence Surveillance Act created a secret court to provide court orders for wiretapping in national security cases.
 - Originally intended to deal with foreign espionage
- Allows warrantless surveillance of non-Americans within the US.
- Allows warrantless surveillance of Americans for 72 hours.
 - Court order must be obtained afterward.

FISA Expansion

- The PATRIOT ACT expanded FISA to also include terrorism on behalf of groups not connected with a foreign government. (i.e. al-Qaeda)
- Violating this law is a felony criminal offense.
- The Constitutionality of FISA has not been clearly established.

FISA sidestepping

- In December 2005, the New York Times revealed that the NSA had been engaging in warrantless wiretapping of individuals alleged to have some sort of connection to al-Qaeda.
- This was authorized by the White House
- Details of the case are mostly secret at this point - it's not known who was monitored or why.
- 2006 - the EFF files a class action lawsuit against AT&T on behalf of customers.

Current status

- Bush has argued that the Constitution gives him the authority to conduct warrantless wiretapping as part of his duties as Commander in Chief.
- In response Congress prepared legislation allowing broad surveillance of non-Americans without a warrant.
- Oversight only after the fact.
- Immunity also provided for telecommunication companies who cooperated in previous wiretaps.
- As it stands, the government has broad authority to surveil non-Americans.
- Powers regarding Americans (including legal residents) are less clear.

Wiretapping

- It appears that two types of wiretapping took place.
- Telephone wiretapping.
 - Phone numbers that were thought to be associated with terrorism were monitored.
- E-mail monitoring
 - E-mail traffic was monitored for “suspicious” phrases and content.

USA Patriot Act

- After 9/11, the US Congress passed the USA PATRIOT act.
- Extended and consolidated surveillance powers.
- Some changes permanent, others have a “sunset” clause.

USA Patriot Act

- Some of the changes in the Patriot Act:
- Increased wiretapping ability
 - Pen registers can be used to track email addresses and URLs. Probable cause is not required - standard is that information is 'relevant to an ongoing criminal investigation.'
 - Nationwide jurisdiction - a judge in New York can issue a warrant to surveil an individual in California.
 - Roving wiretaps - agencies are given more ability to do intelligence gathering without judicial oversight.

USA Patriot Act

- Some of the changes in the Patriot Act:
- Search and seizure:
 - Warrantless search in cases where serving a warrant 'may have an adverse effect.'
 - May seize property that 'constitutes evidence of a criminal offense' (not necessarily terrorism).

USA Patriot Act

- Some of the changes in the Patriot Act:
- Gathering of private information:
 - Easier to collect records from libraries, churches, hospitals, colleges, etc.
 - Standard: 'related to an ongoing investigation' (not probable cause)
 - ISPs may be compelled to give up information about their users.
 - Surveilled individuals not notified.

Concerns

- Arguments in favor of the PATRIOT ACT:
 - Law must catch up with modern technology
 - Reduces barrier to information sharing between agencies.
 - Much of this is already available for prosecuting drug crimes; extends law to terrorism

Concerns

- Arguments against the PATRIOT ACT:
 - Could be used to suppress unpopular opinions (chilling effect)
 - 'pen register' tracking of URLs is more powerful than phone numbers.
 - Roving wiretaps are too broad
 - Evidence seizure can be misused.
 - "Fishing expeditions"

Arguments about the PATRIOT ACT

- What do you think about the following arguments?
 - “You can’t trust the government to use this power responsibly.”
 - “If you haven’t done anything wrong, you have nothing to hide.”
 - “We need to give up some privacy in order to be safe.”
 - “These things are only being used against terrorists.”
 - “Innocent people might be prosecuted or surveilled.”

Discussion

- We seem willing to provide different amounts of personal information to different types of people. This is sometimes called a “ladder of privacy.”
- Sketch out your ladder of privacy. Who do you share extremely personal information with? Publically available information? Anonymized information? None at all?