

63.135 Information Technology and Society

Topic 3: Security and privacy

1. Crime, law enforcement, and IT
2. Definitions and theories of privacy
3. Privacy issues raised by IT
4. Proposed protections

Readings: Baase, Chapters 2 and 5

Inquiry

- Is privacy about power?
- Do IT-enabled security and privacy intrusions assert *power* over individuals?
- Do privacy protections protect the power of individuals?

Objectives

- 3a. Explain issues raised by IT related to security and crime
- 3b. Discuss issues of privacy in the IT era
- 0e. Support opinions by evidence
- 0f. Acknowledge counter arguments

1. Crime, law enforcement, and IT

- Some crime is *computer assisted* or *targets computer use*
- Computers assist in law enforcement
- Law enforcement methods:
 - Interviews
 - Gathering of physical evidence including search and seizure (requires consent or a court order)
 - Surveillance (may not require a court order)
- IT has raised new issues of security and privacy

Financial computer crime

- *Identity theft*: Identifying information is used by thieves to set up false accounts
- *Credit-card fraud*: Card number and ID information are stolen and used to activate card use
- *Stock fraud*: Fraudulently touting stocks one is selling, undervaluing stocks one is buying

Other computer-enabled crimes

- *Auction fraud*: Shill bidding, failure to ship, sale of illegal items
- *Click fraud*: Padding figures for clicks received under pay-per-click advertising
- *Digital forgery*: Using high-quality printers to forge documents

Malicious Internet activity

Intrusion (sometimes called “hacking”): Intruders may read or change files, including Web sites, after guessing passwords or obtaining them by deception

Worms: self-starting programs that harmfully affected Internet computers

Email and other viruses: self-propagating programs that have done billions of dollars in damage

Denial of service attack: Huge numbers of requests for web pages that overwhelm a server

Sexting

- *Definition*: texting, emailing, or posting of sexual self-expression (text, sound, pictures, or videos)
- Sexting of images of *minors* is treated by law enforcement agencies as manufacture, possession, and dissemination of child pornography
- Sexting by adults raises questions of privacy, integrity of relationships, and professionalism

Enforcement approaches

- Computer Fraud and Abuse Act, 1986:
Addressed intrusion, viruses, denial of service
- USA PATRIOT Act increased penalties, broadened definition of terrorist acts, allowed government monitoring without court order
- Cybercrime Treaty (U.S. and Council of Europe, 2006): law-enforcement cooperation; dual criminality (only acts that are crimes in both countries are covered)

Search and seizure of electronic data

- Search requires warrant with specifics
- Seizure of evidence not related to warrant is allowed only if “in plain view”
- What is “plain view” on a laptop?
- Automated search is a grey area

Search and seizure of electronic devices

- Based on court warrant, law enforcement may seize all electronic devices in a place known to contain evidence of crime
- *Example:* child-porn images.
- Seizure may be for search and deletion
- To ensure deletion of content, law enforcement may wipe clean disks or may destroy media

4th Amendment to U.S. Constitution

“The right of the people to be secure in their persons, houses, paper, and effects, against unreasonable search and seizure, 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 and things to be seized.”

2. Definitions and theories of privacy

Privacy-related concerns

- Freedom from intrusion
- Control of access to information
- Freedom from unreasonable surveillance

Aspects of privacy

- *Solitude*: Freedom from disturbance, within reason
- *Anonymity*: Acting publicly without being identified
- *Intimacy*: Private association with others
- *Reserve*: Control of access to personal information
- *Other concerns*: Privacy in different environments; privacy of location; of body, of communication

Two definitions of privacy

- *Control theory* (Fried; Rachels):
One has privacy if one has control of information about oneself
- *Restricted access theory*
(Allen; Gavison): One has privacy if access to information about oneself is restricted

Theories of privacy

- All-or-nothing (have/don't have)
- Repository of information that can be eroded
- Zone that can be invaded
- Confidentiality or trust
- "Being left alone" (Warren and Branden, 1890)

Privacy in the public realm

- Privacy is seen as protecting integrity of an individual's personal sphere
- U.S. Constitution prohibits unreasonable search and seizure, self-incrimination; protects freedom of conscience
- *Lotus Marketplace: Households* was a CDROM with 120 million records of U.S. households, including spending habits
- Outcry about *LM:H* showed gap created by IT between legal-philosophical theory and moral norms about privacy

Communitarian vs. liberalistic ideas about privacy

- *Communitarianism* tends to reject moral right to privacy, accepts greater access to personal data by society: "What do you have to hide?"
- *Liberalistic* view elevates the autonomous self: "Leave me alone"

Free market vs. consumer protection

- Both approaches value privacy, prefer different means to ensure it
- Free-market view emphasizes freedom of individuals to make voluntary agreements and responsiveness of the market; as opposed to political guarantees
- Consumer-protection view emphasizes weak position of consumers relative to vendors: Can an individual realistically negotiate a fair contract with a corporation?

Privacy landmarks

- 1928: Supreme Court decision allowing wiretapping because it involved search and seizure of conversations, not material things
- 1936: Creation of Social Security numbers, expanded later to be taxpayer IDs and for other uses
- 1974: Privacy Act requiring that federal government records be “relevant and necessary” to designated purposes, allowing access and correction by subjects, requiring consent for disclosure to others
- 2001: USA PATRIOT Act loosening restrictions on National Security Letters (for warrantless searches)

Two unusual views of privacy

- (Brandeis, Warren, 1890): Privacy needs special protection; people have a right to legal protection from disclosure of any strictly personal information in print, including gossip
- (Thomson, 1975): Privacy as such does not require protection, because objectionable violations of privacy are also violations of already-protected rights

3. Privacy issues raised by IT

Why issues are raised

- Ease of copying
- Ease of communication
- Ease of collecting data
- Power of processing data
- Storage capacity

Concerns

Protection of data

- *about* a person
- *owned by* a person

Data

- collection
- integrity
- access
- protection

RFID tags

- Small devices with an electronic chip and an antenna, including ID data
- Used to track individual products through manufacturing process
- Easily readable and copiable
- Government has had plans to use RFI in ID documents such as passports

Workplace surveillance and privacy

- Electronic Communications Privacy Act, 1986, expanded prohibitions on unauthorized surveillance
- Exception: monitoring permitted of communications in ordinary course of business, e.g., company email
- Asymmetry of employer-employee power is an issue
- Two viewpoints about workplace privacy begin from (a) fairness; (b) utilitarianism

Issues in use of consumer data

- Customer knowledge of data collection
- Customer knowledge of profiling
- Secondary use
- Opt-in or opt-out
- Accuracy
- Use by law enforcement
- Loss (leakage) by possessor

Why data collection and storage affect privacy

- Online data is collected and linked to computers
- User is often uninformed of collection
- “Secure” data may be leaked
- Large quantities of small information items can reveal more
- Re-identification of “anonymous” data is possible, e.g., queries about one’s car make, sicknewss, college, etc.
- Data online is copied and re-published even if removed
- Data provided for one purpose is often used for other purposes

Data collection

- *Secondary use*: Use of personal information for purposes other than those for which user provided it
- *Computer matching*: Comparing and combining information from different databases, using identifying information
- *Data mining*: Analyzing and searching databases to find patterns and to enable analysis
- *Computer profiling*: Predicting behavior of individual based on data analysis

Opt-in or opt-out?

- How data (e.g., customer information) is used is set by an organization's *privacy policy*
- An *Opt-in* policy means that before data collected about a person is distributed, the person must affirmatively choose that option
- An *Opt-out* policy means that a person will participate unless she/he chooses not to

Knowledge discovery and data mining

- 3 phases: warehousing, mining, interpretation
- *Goal*: discovery of unforeseen patterns
- *Profiling* defines groups of people, with effects on how they are treated
- *Categorical privacy*: a right of individuals not to be profiled as group members based on personal data
- This discussion is made necessary by developments in IT

Who owns the information about a transaction?

- Is a transaction a fact about one party or the other or both?
- Do both parties have the right to make the transaction public or otherwise share information about it?
- Do both parties have the right to expect non-disclosure?
- **Do one customer and a large corporation confront each other in a transaction as equals?** Free-market view says yes; consumer-protection view says no

4. Proposed protections

Processing of personal data

- Directive 95/46/EC of European Parliament, 1995
- *Some provisions:*
 - Data quality
 - Legitimacy of purpose
 - No processing of “sensitive” data (ethnic, political, religious, trade-union affiliations)
 - Right of user to be informed and to correct errors
 - Use for intended purpose

European actions on right to privacy

- European Conference for Protection of Human Rights and Fundamental Freedoms, 1950: Respect for private and family life, home, correspondence
- European Commission of Human Rights, 1976: right to respect for private life is right to privacy requiring legal protection
- OECD data flows guidelines, 1980: 8 principles
- OECD Ministerial Declaration on the Protection of Privacy, 1998

Preventing computer crime

- *Firewall software* monitors incoming communications to filter out suspicious packets
- Credit-card numbers are not printed in full on receipts; only last 4 digits
- Third-party services like PayPal protect credit-card info from untrusted vendors
- Other methods:
 - Not storing unnecessary data
 - Encryption
 - Biometrics
 - Authentication of customer ID

Encryption

- Hides data in plain view
- *Example:* Credit-card numbers may be transformed over Web to be unreadable except by intended recipient
- A *key* (similar to a password) is used to *decrypt* an *encrypted* message
- One application: Digital signatures authenticate the act of accepting an agreement
- Encryption and decryption are performed with *algorithms* developed using mathematical *theorems*

Litigation

- *Responsibility to prevent access:* A legal principle that requires publishers to ensure that material that is illegal in some countries is inaccessible there
- Are libel cases to be tried in country where information is published, or in country where damage is done?
- *Authority to prevent entry:* A country may act to block material that is illegal in that country, but not to block material that is illegal somewhere else

Case: wire tapping

- The September 2010 news article, “US wants stronger wiretap powers over Web,” reports that law-enforcement officials asked Congress to require that all communications-enabling services, be able to intercept communications content for surveillance purposes.
- Critics said that the proposal put in question fundamental aspects of Internet use.
- Give technical and security reasons supporting the request, and give reasons for challenging it.

Key concepts

anonymity	encryption	restricted access
categorical privacy	firewall	theory of privacy
click fraud	Fourth Amendment	RFID
communitarianism	free-market view	search warrant
computer profiling	identity theft	secondary use
consumer-	intrusion	seizure of evidence
protection view	intended purpose	sensitive data
control theory of	legitimacy of	USA PATRIOT Act
privacy	purpose	virus
Cybercrime Treaty	liberalistic view	warrant
data mining	opt-in	
denial of service	plain view	
digital forgery	probable cause	

References

S. Baase. *A Gift of Fire*, 3rd ed. Pearson Prentice Hall, 2008.

M. Castells. *Rise of the Network Society*, 2nd ed. Blackwell, 2000.

R. Spinello and H. Tavani, ed. *Readings in CyberEthics*, 2nd ed. Jones and Bartlett, 2004.

Giannis Stamatellos. *Computer Ethics: A Global Perspective*. Jones and Bartlett, 2007.