

63.135 Information Technology and Society

## Topic 2: Crime, security, and privacy

1. Crime and surveillance
2. Definitions and theories of privacy
3. Privacy issues raised by IT
4. Issues in use of consumer data
5. Solutions

### 1. Crime and surveillance

#### Malicious Internet activity

- *Intrusion* (sometimes called “hacking”): Intruders may guess passwords or obtain them by deception; may read or change files, including Web sites
- *Worms*: started 1988 when a student-installed program harmfully affected several thousand Internet computers
- *Email viruses*: Melissa, 1999, infected a million PCs; Love Bug, 2000, did about \$10B damage
- *Denial of service attack*: Huge numbers of requests for web pages overwhelms servers

## 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

## 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)

## 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

## 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
- *Stock fraud*: Fraudulently touting stocks one is selling, undervaluing stocks one is buying
- *Digital forgery*: Using high-quality printers to forge documents

## Search and seizure of laptop 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

## Litigation

- *Responsibility to prevent access*: A legal principle that requires providers of material to ensure that material that is illegal in some countries by 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

## 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
- Ordinary-course-of-business exception: permits monitoring of communications technology used in ordinary course of business, e.g., company email
- Asymmetry of employer-employee power is a factor
- Two viewpoints about workplace privacy begin from (a) fairness; (b) utilitarianism

## 2. Definitions and theories of privacy

### Aspects of privacy

- Freedom from intrusion
- Control of access to information
- Freedom from surveillance
- Why desired? **Hypothesis:** Privacy limits the *power* of the intruder, information access controller, or surveiller over us

### 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)
- Control, restricted access

## 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

## 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

## 4<sup>th</sup> 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.”

## 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 (enabling warrantless searches)

## Communitarian vs. liberalistic ideas about privacy

- Communitarianism rejects moral right to privacy, accepts greater access to personal data by society
- Liberalistic view of the autonomous self is rejected by communitarians
- IT can blur boundaries between “spheres of access” associated with social roles

## 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
- Market is seen as superior to political system in addressing consumer needs
- Consumer-protection view emphasizes weak position of consumers relative to vendors
- Can individual realistically negotiate a contract with a corporation?

## Two unusual views of privacy

- (Brandeis, Warren, 1980): 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
- *Pro*: “Leave me alone”
- *Con*: “What do you have to hide?”

## Why data collection and storage affect privacy

- All 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

## 4. 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

## 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

## 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

## 5. Solutions

### 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 to be informed and to correct error
  - Use of intended purpose

## 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* and *encrypted* message
- One application: Digital signatures authenticate the act of accepting an agreement
- Encryption and decryption are performed with *algorithms* developed using mathematical *theorems*

## References

- S. Baase. *A Gift of Fire*, 3<sup>rd</sup> ed. Pearson Prentice Hall, 2008.
- M. Castells. *Rise of the Network Society*, 2<sup>nd</sup> ed. Blackwell, 2000.
- R. Spinello and H. Tavani, ed. *Readings in CyberEthics*, 2<sup>nd</sup> ed. Jones and Bartlett, 2004.