PRIVACY

- $\exists$ 3 primary aspects to privacy:
  - freedom from intrusion, being left alone
  - control of information about oneself
  - freedom from surveillance
- We voluntarily cede some degree of the above 3 aspects in order to better interact with strangers.
- Public awareness and concern re. privacy increasing annually.

- concern regarding how personal info is collected, used, and protected

- *personal information* [*PI*]: any info. relating to or traceable to an individual person.

- Computers are not necessary for the invasion of privacy.

  - they do facilitate the collection, analysis, storage, access and distribution of [personal] information.

    * faster and more anonymous searching of DBs

    * gov. & private [commercial] DBs

    * some info. not generally collected heretofore

* difficult public record search facilitated

* info. from diff. DBs combined

Privacy Risks

- invisible information gathering
- unauthorized use [abuse] by info. maintainers
- info. leakage via negligence
  - careless distribution
  - data spillage: PI is sent to advertisers as unintended side-effect of info. & connectivity SW complexity
  - intrusion

  - *secondary use*: use of info. for a purpose other than the one for which it was supplied

- error [misinformation] propagation
  - persistent
  - damaging

- Public Safety VS individual's right to privacy

Big Brother

- Federal intrusion
- databases
- intrusion via *matching & profiling*
  - *matching*: combining & comparing info. from different DBs
  - *profiling*: categorization and assignment of tendency and risk to a group of people indexed in DBs based on common characteristics

    * "fishing expeditions": presumed guilt

  - Computer Matching & Privacy Act [1988]: requires gov. agencies to follow a review process prior to matching. {evidence of lax compliance}

- Should the gov. be allowed by buy PI from private (commercial) DBs that the gov. is constrained from collecting itself?

  - What if some of that info., collected for other purposed is not trustworthy?

  - E.g. ChoicePoint: >10G records for >35 gov. agencies

- location monitoring & tracking

- government privacy abuse is more serious and dangerous because of:
  - its power to demand information unconditionally
  - its mass of data and breadth of DBs
  - personal risk of liberty as well as privacy
  - bureaucratic righteousness and insulation from corrective forces
  - additional access to business DBs

  - absence of statutory due process
  - e.g.
    * IRS (info retrieval & matching including commercial sources),
    * FBI (DB requests from non-criminal agencies)

- Census (used for populating US WW2 internment camps; draft in WW1; zoning violations)
- corporate misuse of law enforcement (e.g. P&G)
- If info is collected, it will most probably be used for many purposes not intended at project inception

4th Amendment & the expectation of privacy

- $\Rightarrow$ no unreasonable search and seizure
- DBs allow search sans court order
- certain laws permit circumvention of court order for some DB searches.
- 2001: weakening of 4th Amendment on many fronts
  - e.g. USA PATRIOT Act

- satellite surveillance and thermal imaging: OK & not OK respectively
- automated toll collection
- itemized purchase records
- Supreme Ct.
  - [1928] Olmstead v. U.S.: no wiretaps
  - [1967] Katz v. U.S.: applies to people not places
  - "reasonable expectation" of privacy {flawed?}

- Electronic Body Searches

- photo DBs:
  - driver photos
  - event attendance {e.g. Superbowl}
  - face recognition
  - 500K CCTV cameras in England

- Fighting Terrorism
  - not a panacea

– countermeasures can be effective

Issues

- *inordinate* expense for innocent to defend selves
- how far can the gov. snoop?
- privacy VS law enforcement
- are we protecting bad law & gov. power abuse (Watergate)
- presumption of *innocence* replaced by presumption of *guilt*

- severe weakening of US 4th Amendment protections against *unreasonable search & seizure* – requirement of *probable cause*

- SSN as Fed. & universal PIN
  - intended use *only* by SS Admin.
  - then IRS taxpayer ID
  - then succession of other erosions
  - not unique – a SSN does not uniquely identify a person
  - more than 60% cards issued on unverified info.
  - know when to withhold your SSN
- National ID cards

- currently proposal only
- integrating many personal data, characteristics, & functions including financial & medical
- benefits:
  - actual card used for verification
  - harder to forge
  - one card only – not several
  - reduction in ID fraud
- hazards:
  - characteristic of totalitarian government

* anti - immigrant
* potential loss of freedom to work
* license to exist

Cause for Concern?

- Who guards the guards
- individual reactions range from indifference to extreme opinions both for and against
- issue of institutional trust
- Privacy Act of 1974 regulates Fed. use of personal data
- routine lack of compliance by Fed. agencies

- many loopholes
- weak enforcement
- poor oversight
- poor security (leakage, selling of info., political snooping, falsification of data)
- ignorance of DB info use
- different solutions for government VS private sector

- government must meet a higher standard

- Jefferson: “eternal vigilance is price of liberty”

Consumer Information

Databases and Marketing

- personal info in mailing lists and related DBs
- USPS COAs provided to mailing list managers & mass mailers
- *data mining*: SW analysis of consumer data
  - used to generate new and maintain previous customers
  - First: consumer profile generated

  - Then: search of DBs to match specific profile
  - *spam* can then be targeted

- *invisible information gathering*:
  - consumers frequently unaware of personal info entry into DBs

- *secondary use*:
  - info used for other purposes than one for which supplied

- What price are we paying for a "free" Web?

- info compiled may be inaccurate, embarrass, or endanger
- dossiers on virtually anyone can be quickly compiled from online sources
- virtually any personal info may be purchased
- consumer business DBs often subpoenaed during litigation
  - customers not informed despite right to challenge
- Children on the Web

- info accessible to potential molesters

- collection of info sans consent { which children can't give}

  – Children's Online Privacy Protection Act [2000]: Web sites must have verifiable parental consent for info. collection

Mass Mailings

- junk mail & spam
- largely nuisance
- privacy suits for junk mail have failed
- $\exists$ Some international and US state laws against SPAM, but no federal (but many proposed)
- Dilemma: we want to announce our services & causes

Credit Bureaus

- Experian, Equifax, & Trans Union
- info can be inaccurate
- federally regulated
- Fair Credit Reporting Act (1970) restricts access
  - easy to circumvent for misuse
  - limits age of negative info

- bad report damaging

- info sold to mailing list compilers
  - neighborhood targeting of advertising
    - discriminates against rich and poor
  - stopped only recently by all CBs [2001]
  - header info can't be sold sans consent [2001]

- Proposed further restrictions
  - consumer right to free copy of own report

– employers need permission to obtain employee report and only for specific job categories

Medical Records

- very sensitive personal info
- little actual legal protection for confidentiality
- existing laws confusing ambiguous patchwork
  - laws both prohibit and mandate disclosure
- Congress: existing laws inadequate (especially since info regularly crosses state lines)

- unauthorized access
  - $\exists$ underground traffic in personal medical info
  - collected for med. product marketing
- HMOs: patient record systems vulnerable to various risks
- medical institutions adopting own privacy policies
- indirect payment for care diminishes our control
  - private insurance
  - Medicare

- medical records may be available to insurers, employers, and the government

- some patients ensure that they minimize their recorded medical info. at greater expense or risk to their health

- public health and research programs require accurate health statistics

- Larger medical care providers & hospitals are replacing paper medical records w. computer DBs. – can be better if access controls used

Proposals:

- Federal DB on health & personal info
  - risks: access possible by more people who are distant, fewer options, easier access by law enforcement etc., denial of care possible if errors
- reporting to national health DB all medical visits
- national electronic health ID card for eligibility and health data storage & access
  - risk: might be used as a national ID card

Tech & Management Solutions for Privacy

- there should be several protections:
- each person w. access needs unique ID w. PW
- hierarchy of access to data and/or operations
  - can improve security over paper
- *audit trails* – tracking of all accesses
- trusted 3rd parties for access

- avoid SSNs as IDs
- encryption – especially for network transmissions
- destruction of obsolete records
- restriction on functions of DB

NOTE: attempts to solve problems generated by a new technology by preventing its use are not likely to succeed.

Awareness

- risks better known by public
- privacy-enhancing technologies
- audit trails
- secure access
- trusted third parties

- consumers paid for their info
  - preys on less affluent?
- privacy audits of Web sites
- chief privacy officer
- TRUSTe
- economic influence by ethical large corps.

The Value of Privacy

- necessary for human dignity, individuality, liberty, and the pursuit of happiness
- essential for intimacy
- allows fraud & deception and hides wrongdoing

Rights to Privacy:

- An independent right to privacy not originally recognized

- Brandeis: is distinct from other rights – needs greater protection

- usually, if privacy is violated, other rights are violated as well

- Brandeis: *inviolate personality*

  – $\exists$ important aspects of privacy not protected by laws against slander, libel, or defamation

  – copyright, contract and property law do not sufficiently protect privacy

  – allowance for news (general interest), limited situations concerning others' interests, and limited dissemination

- how is info used

- Thomson: right to privacy?
  - privacy rights are implicit and concomitant with existing property rights
  - $\exists$ no violation of a privacy right exclusive of violating some other existing right and protection
  - we may waive property rights – intentionally or inadvertently
  - how is info obtained

- Criticisms

- of Brandeis: no workable principles or definitions – too broad a notion, conflicts with freedom of press etc.

- of Thomson: one can argue for cases where privacy *only* has been violated

- neither refutes the other – different emphases

Application of theory to DBs

- Brandeis: *publication* is the objectionable action against privacy
  - *access* and/or use by others to your info. not precluded
- *consent* negates any privacy violation

Economic Viewpoint (Posner)

- Info has both economic & personal value

- one should retain privacy rights if:
  - info is expensive to discover, create , or collect (e.g. trade secret)
  - high personal value but low public value (e.g. nudity)
  - conversations and communications
- but not if:
  - information whose concealment aids in misrepresentation, fraud or manipulation.
- current trends:

  - not following Posner closely
  - more protection for individuals' facts & communications
  - less for organizations

- critics:
  - property rights should follow from moral rather than economic principles

Transactions and Privacy

- multiple parties are involved in transactions

- which has the greater right to privacy?

- if confidentiality agreement made, both parties should honor it

Guidelines for Information Usage

- various organizations, public & private, have developed guidelines for handling personal info.
  - laws or policy recommendations

- Code of Fair Info Practices (1973)
  1. There should be no systems whose existence is secret
     - (should be strengthened to include periodic notification)
  2. There should be a way for a person to find out what data about them are in the system and how they are used

3. Info obtained for one purpose should not be used for another without consent

4. There should be a way for a person to correct errs in their files

5. organizations are responsible for the reliability and security of the data they create, maintain, use or distribute

- the above guidelines are general and widely accepted
  - controversies spawned when adding specificity and the power of law

Informed consent

- when notified by an organization about what info is collected and its usage, consumers choose degree of consent for use

- *Opt out* option: consumers *choose* blanket denial of consent [default: consent]

- *Opt in* option: consumers choose blanket consent [default: no consent]

- *Opt in for each use*: consumer consent required for each use and disclosure of info [default: no consent]

Data Ownership

- can we *own* our personal information?
- (qualified) Yes: likeness (image, voice, etc)
- ???: profile
- consumer awareness, preference and action powerful influence on corporate policy
- advocates recommend annotating medical info waivers to include relevance, expiration, and recipient qualification

Free Market View

- privacy problems solved via market & contract
- motivated by:
  - diversity of values & preferences
  - market response to consumer preference
  - flaws of detailed or restrictive legislation and regulation
- Freedom of Information Use Guidelines

1. Truth in information gathering
    - incorporates informed consent
    - implies liability for violations
2. Freedom in information *contract*ing
    - consumers can voluntarily cede privacy in exchange for a specified benefit
3. Freedom of speech and commerce
    - there should be no external restriction on disclosure of legally obtained info.

Consumer Protection View

- motivation: corporations are more powerful than individuals
- privacy considered more a right than a commodity
- standards change between small & large community
- waivers of confidentiality can be coerced
- free market offers too few protections for consumers & employees

- expectation of average consumer to understand implications of consent is unrealistic
- arguments to consumer of benefits of consent often inflated or misrepresented
- risk outweighs marginal benefit