Privacy and the Use of Information Systems

Harlan J. Onsrud
Department of Spatial Information Science and Engineering
University of Maine

Why should we protect personal information privacy?

What societal benefits do we gain by protecting privacy?

SOCIETAL IMPORTANCE OF PERSONAL PRIVACY

Literature lists many benefits:
(Simitis 1987, Graham 1987, Post 1989; Wacks 1989; Trubow 1990; Rotenberg 1991 and 1993; Reidenberg 1992; Tuerkheimer 1993, and on & on …)

- critical to maintaining tenable democratic societies in a modern world.
- social control through information systems is indeed a real threat

- essential to preserving constructive social and community interactions
- pervasive collection leads to a society that promotes homogeneity by discouraging actions that are perceived negatively by the majority.

- rampant collection increases likelihood of a "...conformist, robotic public seeking to avoid exposure to the risks inherent in functioning in society"
- pervasive collection creates 'chilling effect' on our willingness to deviate from the norm and on our willingness to question authority.

- the purpose of such compilations is to manipulate the individual, not to improve the ability of the data subject to act and decide.

- awareness that minute records of activities are being recorded is by itself probably enough to influence behavior and hinder the discourse of individuals

- social worth becomes increasingly measured by data profiles rather than through personal interactions - human dignity is lost.

- **diversity** in opinions, perspectives, and experiences **promotes innovative ideas** and yet the productivity resulting from diversity decreases in a society in which detailed databases have the effect of decreasing risk taking by individuals.

- over time, inability to control information about ourselves will make us passive citizens rather than active participants in society.

- information privacy is the price that must be paid to secure the ability of citizens to communicate and participate

- those who lack the resources, knowledge, or will to conceal their private and financial lives will be coerced into a position of avoiding controversial or unpopular activities

- based on their unfavorable recorded profiles, many will be excluded from sharing in certain economic and social benefits.

Counter Positions:

- dangers of detailed databases are greatly exaggerated, far-fetched, and unlikely to affect the fabric of American democracy.

- benefits to be gained through responsible use of databases far outstrip the largely subjective and non-quantifiable rights in personal privacy.

- abuses in use should be controlled but not data collection itself.

- far more beneficial for society to deal with privacy abuses on a case by case basis than to restrict database building and the economic efficiency benefits deriving from expanded databases

Code and Other Laws of the Internet (Lessig) p.146

Conceptions of Privacy
- privacy to minimize burden
- privacy as dignity
- privacy as substantive

Which conception(s) should law protect?

How invasive of privacy are geographic information technologies compared to others?

1. geography/location a powerful tool for data integration
2. G.I. technologies powerful tools for tracking, storing, and analyzing personal information (spatial/statistical analysis)
3. detailed local information for business applications fastest growing and potentially most lucrative segment of GIS industry
4. location based services greatly expanding widespread tracking
5. sale of geographic data by state and local governments escalates privacy concerns

Conclusion: lifeline tracking, data integration capabilities and analysis capabilities give GI technologies potential to be **more invasive** of personal privacy than many other technologies

Privacy and IS Technologies

A. Public Databases

Right of Privacy

"...right to be let alone."

Warren and Brandeis, "The Right to Privacy", 4 Harv L Review 193, 1890

Common Law

1. Prevents government interference in intimate personal activities

2. Also prevents intrusions by private individuals

> "... wrongful intrusion into one's private activities, in such a manner as to cause mental suffering, shame, or humiliation to a person of ordinary sensibilities."
> Shorter vs. Retail Credit

3. Refinement by Prof. Dean Prosser into four classes

1. appropriation
2. intrusion
3. public disclosure of private facts
4. false light in public eye

- Based on conflicts involving individuals

- Privacy conflicts in computer age often affect everyone

Legislation

1. 1974 Federal Privacy Act
<http://www.legal.gsa.gov/topicalp2.htm>

a. records on individuals by federal agencies must be for a lawful and necessary purpose
b. provide adequate safeguards against misuse
c. individual can:
- find what information is being collected
- prevent use of the information for other purposes - - no longer true, inform rqmt
- access, copy, and make corrections

2. Other Federal Legislation

Fair Credit Reporting Act (1970)
Family Education Rights and Privacy Act (1974)
Tax Reform Act (1976)
Right to Financial Privacy Act (1978)
Privacy Protection Act (1978 - search warrants),
Electronic Fund Transfer Act (1980 - banks must notify you about third party access to accounts)
Electronic Communications Privacy act (1986 - unauthorized eavesdropping and wiretaps)
Video Privacy Protection Act (1988)
……. etc.

3. Similar privacy acts in each State

- apply most often to state and local government agencies

B. Privately Owned Databases

Greatest threat to individual privacy in the U.S. is the private commercial sector!

"Tying data to its geographic location is one of commercial sector's most promising and powerful tools in compiling data from widely disparate sources on households and individuals." (GIS in Business '93)

Why should the IS commercial, government, and academic sectors care about privacy issues?

93% of Americans favor regulations prohibiting sale of information without permission of the subject (1991 Time/CNN Poll) -- consistently above 95% every year

- nuisance factor
- security and safety factor
- societal control factor

"protect privacy" vs. "allow efficient, effective operation of business and government"

How to strike a better balance?

National Decision Systems keeps track of the following data categories on individuals and households:

- address
- age
- ethnicity
- children's ages
- veteran status
- household income
- buying habits
- phone number
- gender
- religion
- smoking habits
- marital status
- dwelling type
- lifestyle category

(Equifax and National Decision Systems 1993 and 1992 a-d)

- available on over 140 million Americans in approximately 100 million households

Typical Current Cross Matching Activities in the Commercial Sector (ten years ago)

- name, address, height, and weight from your drivers license file (allowed in many states)
- scanned image (taken from any available photo identification card)
- ZIP+4 address location provided by the Census Bureau,
- cadastral, taxation, and facilities records provided by local government
- scanned bar-code purchases you make at grocery and other retail stores
- social security number
- hundreds of other electronic databases being used daily to keep track of everything from magazine subscriptions to gasoline purchases

1. Can **common law** right of privacy be expanded to deal with database privacy?
   (i.e. expand to cover conflicts which now affect everyone?)

2. Possible to draft **legislation** to head off most abuses? - purportedly 45 bills in 2001 session of Congress including "Location Privacy" bill

3. Are new laws the answer?

What principles to follow in drawing the line between
permissible exchange of facts in order to support a commercial goal
versus
an impermissible intrusion?

Possible Principles:
* economic efficiency
* current mores regarding human dignity
* "chilling effect" test
* restrict data use in commercial sector to purpose for which collected
* apply federal privacy act provisions to commercial sector
* (?)

Privacy - "the ability of the individual to control information about oneself"

Most basic norms for protecting privacy generally agreed upon long ago (1973 Code of Fair Information Practices (US HEW), 1980 OECD Privacy Guidelines, 1995 Common Position of European Parliament and Council of EU, June 1997 U.S. Dept of Commerce Report - Perritt)

- No personal data record keeping may be maintained in secret.
- Individuals must have a means of determining what information about them is in a record and how it is used.
- Individuals must have a means of preventing information about them obtained for one purpose from being used or made available for other purposes without their consent.
- Individuals must have a means to correct or amend a record of identifiable information about themselves

- An individual whose request for correction or amendment has been denied must be able to place a statement of disagreement into the record
- Limits should be placed on the disclosure of certain personal information to third parties
- Organizations creating, maintaining, using, or disseminating personal data must assure reliability of data for the intended use and take reasonable precautions to prevent misuses
- Individuals must have a means of seeking review of denied requests and remedies for alleged violations of duty
- Data controllers must maintain data and ensure data security.

These principles are NOT legally imposed against the commercial and private sectors in the U.S.

Best way to enforce norms NOT agreed upon in the U.S.

Regulation Models: (Milberg et al, Comm of ACM, Dec 95)
- Each model below may include some of those above it.
- Ordered in increasing levels of government involvement

1. Self Help Model - Purely Private Enforcement
Data subjects have right of access and correction but each must identify problems and bring to courts themselves. Primary burden is on data subjects to challenge inappropriate actions.

2. Voluntary Control Model
Self-regulation on the part of corporate players. Law defines specific rules and places burdens on responsible person in each corporation to ensure compliance.

3. Data Commissioner Model
Commissioner has no powers but acts as an ombudsman. Relys on complaints from citizens. General watchdog and might also provide expert advice.

4. Registration Model
Any entity gathering personal information must register the dataset. De-registration and penalties upon complaint and finding of failure to meet standards.

5. Licensing Model
Prior approval required for any use of personal data.

Alternative Categorization of Regulation Models:
Chief Institutions for Protecting Personal Information
(Swire, June 1997 - Commerce Dept Rpt)

1. Rely on Marketplace
reputation and sales of companies will suffer if they offend customers
- largely what we have now
- businesses quite happy

2. Rely on Government
enforcement of mandatory legal rules by agencies will deter companies from abusing people's privacy

3. Rely on Self Regulation by Industries
self regulatory guidelines by industry groups
- Swire sees this as an appropriate compromise
- privacy advocates generally don't, many want a right to information privacy

Protection of Privacy in Europe

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data

Opened for signatures, Jan. 1981
In force, Oct. 1985

No restrictions in the name of privacy on the transfer of data from the Territory of one Party to the Territory of another.

Provided that, member States ensure through legislation:

- subjects have right of access to records on themselves
- right of correction/disagreement
- data not excessive relative to purpose for which stored
- identity of persons expunged after original purpose for data no longer exists

Data Correction Authority created with power to restrict export under some circumstances
- impose penalties for those who breach

Additionally, at a minimum, those collecting personal data must provide government authority with:

- purpose of the digital file
- descriptions of the types of data the file contains
- name and address of the **controller** of the file
- third parties to whom data might be communicated

- Controllers of data sets only permitted to record and process personal data with the **consent** of the subject (Some narrow exceptions)
- Controllers obligated to take appropriate technological and organizational **security** measures
- Data flows may be restricted to countries that don't provide similar protections

Further Alternatives to European Models
(Perritt, June 1997 - Commerce Dept Rpt)

Enthusiasm for European models has generally abated in U.S. - Why?

- difficult implementation issues - less effective and more difficult than advocates foresaw and, in fact, no new revolutionary rights provided
- we involve government bureaucracies as little as possible or not at all - cultural

European directive is in force which requires that any trading partner outside EU have same level of privacy protections
- trade with U.S. companies possible by contract (Feb 2000)

Alternatives to European Models (Perritt cont'd)

1. Privacy Commission or Privacy Ombudsman
- solely watchdog function

2. Expand Federal Credit Reporting Act (FCRA) to broader classes of traders in information
- transfer to third party requires "legitimate business need for the information in connection with a business transaction involving the consumer"

3. Create an Individual Property-type Right in Personal Information

Problems:
1. commercial value of data collections will be decreased - most informed people with money will opt out
2. many not opting out will want to be paid - increase of costs for products
3. cumbersome and expensive for businesses to administer those opting out or wanting cash for their personal information

• None of the above three models has received widespread support

• Perritt sees #2 as most practical at federal level in U.S.
• Lessig has suggested #3 for serious consideration

4. Self-regulation by Industry
- most touted at current time and largely status quo

Major Concerns: (Perritt)
1. protections won't go far enough in protecting data subjects
2. recalcitrant members of an industry can gain competitive advantage over those that comply
   - self regulation tends to unravel because of cheaters, need benefits that can be taken away
   - remove right to any domain names on the internet for your company?
3. antitrust law - violation of competition law for competitors to combine to set the terms of competition and enforce

Get around by:
- following rules for standard setting under antitrust law?
- following model of collective bargaining? (groups such as ACSM and ASPRS bargain with and obligate their members to standards and principles agreed to by all other major information industry associations)

Conclusions:

No quick or simple solutions in the U.S.

Likely, to see continued patchwork of state and federal statutes and regulations restricting access to and disclosure of personal information in private sector and government databases

Personal bias:

- would like to see a few States give a property right in personal information and let people buy, sell, and self-enforce data about themselves

Privacy web site starting points:

<http://special.northernlight.com/privacy/index.html>
Privacy Links

<http://www.stanford.edu/group/lawreview/symposium/index.html/>
Cyberspace or Privacy: A New Legal Paradigm?

< http://www.cfp.org/>
Conference on Computers, Freedom and Privacy