Privacy and the Use of Information Systems

Harlan J. Onsrud
School of Computing and Information Science
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

Privacy and Information System Technologies

Right of Privacy

"...right to be let alone."

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

Fourth Amendment Privacy Right

- protects against unreasonable searches and seizures
- wording addresses only physical interference with tangible things … "persons, houses, papers, and effects"
- does it or should it extend to personal data and private communications?

Katz v. United States (1967)

- pay phone listening device
- first case heard by Supreme Court involving electronic device impacting right to privacy
- your constitutional right of privacy extends to anyone who has a "reasonable expectation" that their information is private

Kyllo v. United States (2001)

- portable thermal imager used to determine if D was likely growing marijuana. D claimed 4th Amendment privacy right

- S.C. held thermal imaging was an intrusion into the home

- activities behind closed doors are performed with reasonable expectation of privacy

Katz and Kyllo focused on a right to be secure in spatial terms

- warrant and probable cause needed to search one's home
- concept has not been constitutionally expanded to stored data about you … example: data and metadata reported from cookies to elsewhere even if generated while sitting on a computer in your home is probably not covered by your constitutional privacy right
- remains case-by-case determination of reasonable expectations under the circumstances

Further Judge Made Privacy Tort Law

1. You constitutional privacy right 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 tort 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

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 geospatial technologies compared to others?

1. location in time & place a powerful tool for data integration
2. geospatial technologies powerful for tracking, storing, mining and analyzing personal data (spatial/statistical analysis)
3. human location and relations to physical and virtual place over time is the most lucrative and growing segment of commercial sector
4. sale of geographic data by state and local governments exacerbates privacy concerns

Conclusion: Embedded within and supporting lifeline tracking, pervasive sensor networks, data integration, data mining, and AI analysis, geospatial technologies are **more invasive** of personal privacy than most other technologies

Because U.S. Constitutional judge-made privacy law remains murky, state and federal legislatures have stepped up in some instances to provide further clarity, typically on a sector by sector basis.