
Information Privacy

January 15, 1998

Kathy A. Stewart

Privacy

- ◆ What are some things we do to achieve privacy?
- ◆ Physical vs. Informational
- ◆ Why is Information Privacy Important?
 - Psychological Viability
 - Relationship Tool (professional & personal)

Privacy Defined

- ◆ “The right to control personally identifiable facts about oneself.”
- ◆ “The right to be let alone.” (Warren and Brandeis, 1890)
- ◆ “A condition of limited access to identifiable information about individuals” (Smith, 1993)

Value of Personal Information

- ◆ Why are organizations so eager to obtain personal information?
 - increased competitive environment
 - market of “one”
 - better product decisions
 - capabilities of Information Technologies

Examples of Information Practices

- ◆ Psychographic Profiling Enabled by Statistical Modeling
- ◆ Secondary Use vs. Primary Use
 - » sharing (internal or external)
 - » cross-selling information
 - » minute description/computer matching

Corporate Policy-Making

- ◆ Smith (1993) found a reactive approach to policy-making
 - Drift: existing policies conflict with practice
 - » emotional dissonance/organizational mores
 - » incremental “policy by least steps”
 - » lack of executive/industry leadership
 - Threat:
 - » negative publicity
 - » legislative scrutiny
 - Reaction
 - » task force/draft documents
 - » Senior management involvement and official response

Does Privacy “Pay” for Corporations

- ◆ Most consumers enjoy and want the benefits of corporations knowing about them.
- ◆ The real issue is CONTROL.
 - “opt out”
 - ask permission
 - notify of collection/secondary use personal information

Boston Consulting Group Survey

- ◆ Survey Assessed Web visitor and online merchant attitudes regarding privacy and privacy assurance programs.
 - 76% concerned about site's monitoring user browsing on the Internet
 - 70% worried about online purchases
 - 40% of users have provided false information at least once while registering at a Web site
 - 78% say privacy assurance will increase their comfort in providing personal information over the Internet.
 - 63% of users now reluctant to provide personal information say they would divulge information if Web sites disclose clearly how the information will be used.

Boston Consulting Group Study (Cont.)

- ◆ Growth in electronic commerce will be measurably impacted if Web sites do not conform to self-regulation standards.
 - With no action taken to address privacy concern EC will be a \$6 billion dollar business by year 2000
 - With privacy web site policies, however, the industry could double from \$6 billion to \$12 billion

Louis Harris/Westin Survey

- ◆ Of the 58% of users who have been asked to provide information at a Web site, 79% declined and 8% supplied false information.
- ◆ 63% of the decliners/users said they would have divulged information if the site disclosed clearly how the information would be used.
- ◆ 87% of Internet users say it is “very” or “somewhat important” that Web sites with cookies obtain users’ permission before placing the identifier.
- ◆ 43% of computers users who do not use the Internet/online service say that consumers have lost control over how businesses use and circulate their personal information.

Web Privacy

- ◆ *What are some recommended strategies for protecting privacy on the Web?*
 - Write and post the sites privacy policy.
 - Enforce secondary use restrictions (links with other databases? Sharing or selling personal information?)
 - Allow users to create a *personal profile*; allow them to access and update the information they wish to make available.
 - Provide user anonymity when accessing the home page
 - Inform users of ‘cookies’.

Federal Privacy Laws in the United States

◆ General Federal Privacy Laws

- Freedom of Information Act, 1968
- Privacy Act of 1974
- Electronic Communications Privacy Act of 1986
- Computer Matching and Privacy Protection Act of 1988
- Computer Security Act of 1987
- Federal Managers Financial Integrity Act of 1982

Federal Privacy Laws in the United States (cont.)

- ◆ **Privacy Laws Affecting Private Institutions**
 - Fair Credit Reporting Act of 1970
 - Family Educational Rights and Privacy Act of 1978
 - Right to Financial Privacy Act of 1978
 - Privacy Protection Act of 1980
 - Cable Communications Policy Act of 1984
 - Electronic Communications Privacy Act of 1986
 - Video Privacy Protection Act of 1988

Fair Information Practices Principles

- ◆ There should be no personal record systems whose existence is secret.
- ◆ Individuals have rights of access, inspection, review, and amendment to systems that contain information about them.
- ◆ There must be no use of personal information for purposes other than those for which it was gathered without prior consent.
- ◆ Managers of systems are responsible and can be held accountable and liable for the damage done by systems for their reliability and security.
- ◆ Governments have the right to intervene in the information relationships among private parties.

Current Government Initiatives

- ◆ H.R. 98, the *Consumer Internet Privacy Protection Act of 1997*, will require prior written consent before a computer service can disclose a users' personal information to a third party.
- ◆ The FTC plans to conduct a “*computer database study*” to examine personal information held by private companies.
- ◆ The FTC is set to review the practices of top Web sites in March 1998. The FTC is looking for “*demonstrable progress*” among sites to or else government intervention will be probable.

European Government

- ◆ **European Union (EU) Data Protection Directive:** the Directive requires very strict protection of personal information including basic demographics, race, politics, finances, religion, and health.
- ◆ *Companies must ensure that personal information on the Internet is*
 - Processed fairly and lawfully
 - Collected and processed for specified, explicit, legitimate purposes
 - Accurate and current
 - Kept no longer than deemed necessary to fulfill the stated purpose.

European Government (cont.)

- ◆ *User's information privacy rights include:*

- Right to access
- Right of correction, erasure, or blocking of information
- Right to object to usage
- Right to oppose automated individual decision
- Right to judicial remedy and compensation

- ◆ *In addition:*

- before transferring information, companies must ensure an “adequate” level of protection in the recipient country
- EU countries may authorize information transfer to countries with “inadequate” protection if the online company provides sufficient guarantee of users' rights, via contractual clauses.