CURRENT DEVELOPMENTS IN U.S. PRIVACY REGULATION

Harvard Information Infrastructure Project
Kennedy School of Government
Cambridge, Massachusetts

November 26, 2001

Barry J. Hurewitz
Hale and Dorr LLP
Washington, DC

HALE AND DORR LLP

PRIVACY

"The right to be left alone -- the most comprehensive of rights, and the right most valued by a free people."

Justice Louis Brandeis

Olmstead v. United States (1928)

PUBLIC OPINION:
Emerging Values Alter the Privacy Debate

- Privacy ranked as the #1 Internet issue for consumers
  - *Business Week* survey, 1998
- 87% concerned about online privacy invasion
  - AT&T survey, 1999
- 59% want more federal privacy legislation
  - *Business Week* survey, Feb. 2001
- 51% want national identification cards
  - *Fabrizio McLaughlin & Assoc. poll*, Sept. 2001
- 55% prefer enforcement of existing laws over new privacy laws
  - *Fabrizio McLaughlin & Assoc. poll*, Oct. 2001

SOURCES OF PRIVACY REGULATION: A State of Confusion

- Targeted mandatory privacy safeguards
- Industry "self-regulation"
- Governmental surveillance
- Inconsistent state laws
- Emerging global standards
- Administrative policies
- Legislative intervention
- Judicial precedents

- ***"Fair Information Practices"***

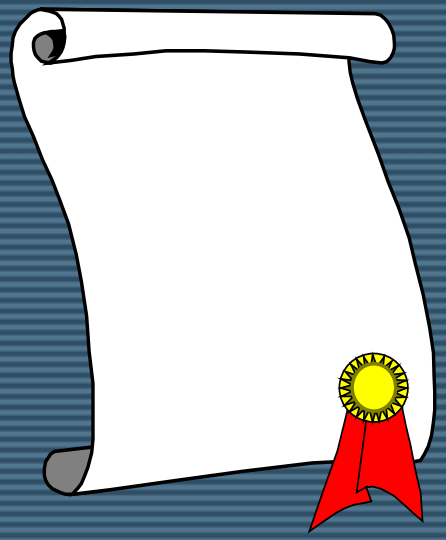
FAIR INFORMATION PRACTICES

Widely accepted principles for centralized management of personal information:

1. Notice
2. Choice
3. Access
4. Security
5. Enforcement

FAIR INFORMATION PRACTICES

1. NOTICE



Before collection, use or disclosure,

Who is collecting data?
What data is collected?
How is data collected?
Why is data collected? (primary uses)
What other uses? (secondary uses and “exceptions”)
How is data protected?
What choices are available?

FAIR INFORMATION PRACTICES

2. CHOICE

Approaches for secondary uses of data:

- Opt-in
- Opt-out
- User-defined preferences

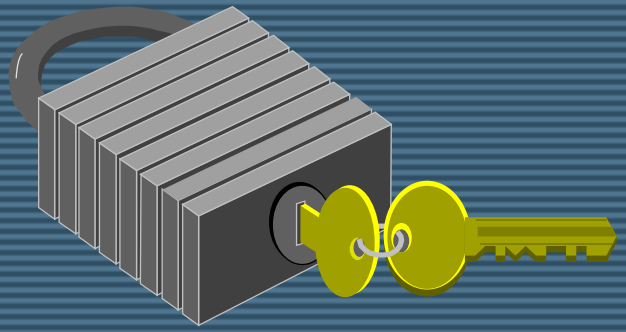
FAIR INFORMATION PRACTICES

3. ACCESS

- Right to view data about oneself
- Right to ensure accuracy & completeness
- Procedures for requesting changes

FAIR INFORMATION PRACTICES

4. SECURITY



Data integrity:

- Use trusted sources
- Update regularly
- Use de-identification

Data security:

- Managerial safeguards
- Technical safeguards
- Physical safeguards

FAIR INFORMATION PRACTICES

5. ENFORCEMENT

- Complaint procedure
- Investigation
- Redress
- Sanctions

FEDERAL PRIVACY LAWS

Federal privacy laws purport to balance competing privacy and information access interests in narrow "sectors"

- Government Records
- Children
- Financial
- Health/Medical
- Communications

FEDERAL PRIVACY LAWS
Government Information

- **Privacy Act** (1974): Limits public access to personally identifiable data in government records
- **Freedom of Information Act** (1974): Creates presumption in favor of disclosing government records, with exceptions for private, proprietary, and investigative information
- **Computer Matching & Privacy Protection Act** (1988): Limits federal agencies' right to share data among separate government databases
- **OMB Cookie Policy** (2000): Requires notice, compelling need, safeguards and high-level approval to use cookies on federal web sites

FEDERAL PRIVACY LAWS
Children's Online Information

- **Children's Online Privacy Protection Act** (1998): FTC rules require notice and consent in order for "operators" of commercial web sites and online services to collect "personal information" from children under 13
- Regulations took effect in 2000
- FTC considers third-party best practices for "safe harbor" acceptance
- April 2001: FTC negotiated civil penalty settlements with three web site operators
- Oct. 2001: Due to lack of new, reliable technologies, FTC proposes to extend use of email consent to 2004

FEDERAL PRIVACY LAWS
Financial Information

- **Right to Financial Privacy Act** (1974): Restricts disclosures by banks
- **Fair Credit Reporting Act** (1988): Restricts disclosures of consumer credit information
- **Gramm-Leach-Bliley Act** (1999): Requires entities "significantly engaged" in "financial activities" with consumers to provide notice of information practices and allow customers to opt-out of disclosures to non-affiliated third parties
  - Rules issued in 2000
  - Existing customers notified by July 1, 2001
  - Data security rules proposed August 2001

FEDERAL PRIVACY LAWS
Health Information

- **Health Insurance Portability & Accountability Act** (1996): Health plans, health care providers, and health care data processing clearinghouses must provide notice and obtain consent (opt-in) for most uses and disclosures of individually-identifiable health information
  - Exceptions for supervised research, public health, law enforcement
  - Extended through contracts with "business associates"
  - Rules issued April 2001, to be enforced April 2003
  - States can adopt more stringent medical privacy laws

FEDERAL PRIVACY LAWS
Communications

- **Electronic Communications Privacy Act** (1986)/ **Omnibus Crime Control & Safe Streets Act** (1968): Generally prohibits private interception of wire, oral, and electronic communications, allowing minimal access needed in order to provide service

- Criminal penalties and private civil damages depend upon the medium of communication and the nature of the violation

- Exceptions allow for government surveillance
  - Probable cause for content intercepts
  - Relevance for non-content subscriber data

FEDERAL PRIVACY LAWS
Communications

- **Computer Fraud & Abuse Act** (1986): Prohibits unauthorized access to a computer to obtain information

- Applies to financial institutions, government systems, or any computer used in interstate or foreign commerce or communication

- Civil and criminal penalties

FEDERAL PRIVACY LAWS
Communications

- **Communications Assistance for Law Enforcement Act** (1994): Requires telecom carriers to ensure that their equipment, facilities and services are compatible with government surveillance technologies, providing:
  - unobtrusive delivery of intercepted communications and
  - call identifying information to the government
- Aug. 1999: FCC mandated compliance for packet-switched communications (call-ID plus content)
- FBI sought "punch list" of additional call data
- Aug. 2000: Court remands technical issues to FCC
- Fall 2001: FBI working on technical standards to facilitate surveillance of ISPs and email

FEDERAL PRIVACY LAWS
Communications

- **Communications Act Section 222**: Restricts uses and disclosures of Customer Proprietary Network Information (CPNI) maintained by telecom service providers
- Covers billing, quantity, location, configuration, type of service, and usage level
- Excludes subscriber list/directory information
- FCC proposed opt-in requirement for "push" marketing uses of non-location data, but Tenth Circuit (1999) found impermissible infringement of commercial speech
- Fall 2001: FCC received public comments on how to revise and/or justify CPNI rules

FEDERAL PRIVACY LAWS
Communications

- **Wireless Communications & Public Safety Act** (1999): Added wireless caller location to definition of CPNI

- Location wireless tracking capability mandated for Enhanced 911 service

- "Express prior authorization" (opt-in) required for use and disclosure of call location information and secondary uses of crash notification system

- Exceptions for emergency services and family notification

FEDERAL PRIVACY LAWS
Communications

USA PATRIOT Act (2001)

- Expands pen register/trap & trace (non-content) authority to all forms of communications
- Added Computer Fraud & Abuse as a basis for wire surveillance
- Added surveillance of voicemail under ECPA
- Added access to IP addresses and Internet session data
- Allows voluntary disclosures by service provider to prevent death or serious injury or to prevent harm to their property
- Requires service providers to disclose "relevant and material" non-content subscriber data, regardless of medium
- Allows "roving" wiretaps for gathering foreign intelligence
- Provides one-stop nationwide authorization for certain federal surveillance
- Does not change CALEA

CURRENT FEDERAL ADMINISTRATIVE ACTIVITY

FCC

- CPNI disclosure standards
- Scope of CALEA

CURRENT FEDERAL ADMINISTRATIVE ACTIVITY

FTC

- May 2000: Call for general federal privacy legislation to supplement inconsistent self-regulation
- Oct. 2001: Withdrew request for legislation to focus on
  - "Buttressing" private enforcement of online privacy policies
  - Children's online privacy enforcement
  - Gramm-Leach-Bliley enforcement
  - Identify theft enforcement

CURRENT FEDERAL ADMINISTRATIVE ACTIVITY

HHS

- Possible revisions to HIPAA privacy rules
- Development of related HIPAA data and security standards
- Possible changes in “common rule” to protect human research subjects
- Genetic privacy

CURRENT FEDERAL ADMINISTRATIVE ACTIVITY

Defense

- Seeking new secure networks, possibly based on peer-to-peer models
- Seeking new surveillance tools and technologies for war on terrorism
- “Echelon”

CURRENT FEDERAL ADMINISTRATIVE ACTIVITY

FBI

- Enhanced access under CALEA
- "Digital Storm" data mining technologies
- "Carnivore" Internet surveillance program

CURRENT FEDERAL ADMINISTRATIVE ACTIVITY

INS

- Enhanced entry-exit tracking under 1996 law

CURRENT FEDERAL ADMINISTRATIVE ACTIVITY

Commerce Department

- International Trade Administration implementation of EU Privacy Safe Harbor program

- Bureau of Export Administration encryption export policy

CURRENT FEDERAL ADMINISTRATIVE ACTIVITY

Various Agencies

- Evaluation of biometric security tools
- Development of new security screening technologies
- Development of imaging and facial recognition tools for use public places

INDUSTRY SELF-REGULATION:

- Sectors without legislated privacy mandates are “self-regulated” (general online privacy)
- Self-regulation does not mean unregulated!
- Fair Information Practices emerging as industry standards
- Companies respond to public opinion (Network Advertising Initiative)
- Emerging technical standards (P3P)
- Foreign laws (EU’s comprehensive Privacy Directive) drive private data policies
- Non-governmental industry organizations (BBBOnline, TRUSTe)
- Private class action lawsuits

LOOKING AHEAD: WHAT'S NEXT?

- Continued concern over new technologies
- Sector-based regulation
- De facto international standards
- Increased reliance on electronic data and networks
- More government surveillance powers
- Higher volume of data traffic
- Improvements in privacy-protective technologies

MORE INFORMATION

Barry J. Hurewitz

barry.hurewitz@haledorr.com

202-942-8413

www.haledorr.com

www.InternetAlerts.net

HALE AND DORR LLP