Whatever Happened

to the

Fair Information Practices ?

Beth Givens
Director
Privacy Rights Clearinghouse

Privacy Symposium

August 22, 2007
Cambridge, MA

Topics

- Definition and origins of FIPs
- Overview of key codes
  - U.S. HEW principles, 1973
  - OECD principles, 1981
  - Canadian Model Code, 1995, & nat'l law, 2000
  - U.S. NTIA's Elements of Self-Regulation, 1998
  - U.S. Federal Trade Commission's FIPs, 1998
  - EU Data Protection Directive, 1998
  - U.S. Safe Harbor Agreement, 2000
  - APEC Privacy Framework, 2005
  - Global Privacy Standard, 2006
  - Sector-Specific Codes – Accountancy and Health
- Conclusions & Resources

About the Privacy Rights Clearinghouse

- Nonprofit organization
  - Established 1992, San Diego, CA
  - Two-part mission: education & advocacy
- Consumer hotline via e-mail and phone
- Consumer guides: 50+ Fact Sheets
  - ID theft, credit, online, telemarketing, medical, employment screening, & more
- Web: **www.privacyrights.org**

What Are the Fair Information Practices (FIPs) ?

- “Fair information practices (FIPs) are a set of principles for defining and addressing concerns about privacy of personal information.”
- “In most countries with privacy laws, [they are the] core privacy principles … incorporated in privacy and data protection laws.”

-- Robert Gellman’s essay on FIPS in *Encyclopedia of Privacy* (2007)

Origins of the Fair Information Practices

An early expression of FIPs is found in the definition of information privacy (1967):

"…the claim of individuals … to determine for themselves when, how, and to what extent information about them is communicated to others."

-- Alan Westin,
Privacy and Freedom (1967)

Origins of FIPs, cont'd.

- Embedded in U.S. Fair Credit Reporting Act (FCRA) of 1970
  - Access to one's own credit report
  - Use limitations
    -- legitimate business purposes
  - Accuracy and correction
  - Recourse if illegitimately accessed and misused

Development of FIPs

Reports in early 1970s

- In Britain, the Younger Committee report – 10 principles (1972)
- Alan Westin & Michael Baker, *Databanks in a Free Society* (1973) -- called for formulation of "codes for record-keeping practices"
- U.S. Health, Education and Welfare (HEW) committee report (1973) *-- Records, Computers, and the Rights of Citizens*

-- Colin Bennett,
Regulating Privacy (1992)

Development of FIPs, cont'd.

- Data protection laws enacted in 1970s – FIPs embedded
  - Concerns over advancement of computer technology and its impact on privacy
  - State of Hesse, Germany (1970)
  - Sweden (first nation, 1973), U.S. (1974), Germany (1977), France(1978)
- Council of Europe Resolutions: '73, '74, '81
- OECD Guidelines -- International code established by Organization for Economic Cooperation and Development (1981)

-- Colin Bennett, *Regulating Privacy*

U.S. HEW Principles (1973)

[Paraphrased]

1. No secret systems of personal data.
2. Ability for individual to find out what is in the record, and how it is used.
3. Ability for individual to prevent secondary use.
4. Ability to correct or amend record.
5. Data must be secure from misuse.

-- Paraphrased from
1973 U.S. Health, Education and Welfare report:
Advisory Committee on Automated
Personal Data Systems

OECD Principles (1981)

"Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"

1. Collection limitation
2. Data quality
3. Purpose specification
4. Use limitation
5. Security safeguards
6. Openness
7. Individual participation
8. Accountability

Criticisms of OECD FIPs

- Some consider them too weak.
- Allow too many exceptions.
- Do not require a privacy agency.
- Have not kept pace with information technology.
- Some industry critics want them reduced to notice, choice, and accountability.

-- Summarized from Robert Gellman's essay on FIPs, *Encyclopedia of Privacy* (2007)

Canadian Standards Assoc.
Model Code for Protection of Personal Information (1995)

- Accountability
- Identifying purposes
- Consent
- Limiting collection
- Limiting use, disclosure, retention
- Accuracy
- Safeguards
- Openness
- Individual access
- Challenging compliance

Incorporated into Canada's nat'l law, PIPEDA (2001)

Emphasis on Self-Regulation in the U.S.

- TRUSTe web site seal program (1997)
- Elements of model privacy disclosures
  - Information collection and use
  - Communications from the site
  - Information sharing and disclosure
  - Choice / Opt-out
  - Log files, cookies, clear gifs, third-party advertisers, links to other sites, co-branding…
  - Access, security, changes in policy

Self-Regulation in U.S., cont'd.

- Online Privacy Alliance -- "Guidelines for Online Privacy Policies" (1998)
  1. Adoption of Privacy Policy
  2. Notice and Disclosure
  3. Choice and Consent
  4. Data Security
  5. Data Quality and Access

U.S. NTIA's Elements of Self-Regulation (Jan. 1998)

Fair Info. Practices

1. Awareness
   a. Privacy policies
   b. Notification
   c. Consumer education
2. Choice
3. Data security
4. Consumer access

Enforcement

1. Consumer recourse
2. Verification
3. Consequences

Nat'l Telecomm's and Information Admin. , U.S. Dept. of Commerce

U.S. Federal Trade Commission
Fair Information Practice Principles (June 1998)

1. Notice / Awareness
2. Choice / Consent
3. Access / Participation
4. Integrity / Security
5. Enforcement / Redress
    a. Self-Regulation
    b. Private Remedies
    c. Government Enforcement

Shortcomings of U.S. Self-Regulatory Approach

- Absence of collection limitation provision
- Absence of use limitation principle
- Self-regulatory environment
- Limited enforcement
- No privacy agency *per se*

European Union Data Protection Directive (Adopted 1998)

Rights of data subjects, including:

- Right of access to data.
- Right to know where the data originated.
- Right to have inaccurate data corrected.
- Right of recourse in the event of unlawful processing of data.

Cont'd.

EU Data Protection Directive, cont'd. (1998)

Rights of data subjects, cont'd.

- Right to withhold permission to use their data in certain circumstances.
- Where data is transferred from EU country to a non-EU country, Article 25:
  - Non-EU country receiving the data must provide an adequate level of data protection.

-- Summarized from Morrison & Foerster Legal Updates, 02/2000

Safe Harbor Privacy Principles

U.S. Dept. of Commerce

(Signed July 21, 2000, Implemented July 1, 2001)

- Notice
- Choice
- Onward transfer
- Security
- Data integrity
- Access
- Enforcement

For use by U.S. entities receiving personal data from the EU in order to qualify for safe harbor and presumption of “adequacy.”

APEC Privacy Framework
Asia-Pacific Economic Coop. (2005)

- Preventing harm
- Notice
- Collection limitation
- Uses of personal information
- Choice
- Integrity of personal information
- Security safeguards
- Access & correction
- Accountability

Global Privacy Standard (2006)

- Consent
- Accountability
- Purposes
- Collection limitation
  - Data minimization
- Use, retention and disclosure limitation
- Accuracy
- Security
- Openness
- Access
- Compliance

Adopted at 28th Intnat'l. Data Protection Commissioners Conference – Nov. 2006

Sector-Specific Codes

- *Privacy Framework*, American Institute of Certified Public Accountants & Canadian Institute of Chartered Accountants (2003) – renamed *Generally Accepted Privacy Principles*
- *Connecting for Health's Policy Principles,* Markle Foundation (2006) – part of Connecting for Health Common Framework

Accountants' Code
Generally Accepted Privacy Principles

- Choice and consent
- Management
- Notice
- Collection
- Use and retention
- Disclosure to third parties
- Quality
- Security
- Notice
- Access
- Monitoring and enforcement

AICPA / CICA Principles, 2003

Connecting for Health's Policy Principles -- Markle Foundation

- Openness and transparency
- Purpose specification and minimization
- Collection limitation
- Use limitation
- Individual participation & control
- Data integrity and quality
- Security safeguards and controls
- Accountability and oversight
- Remedies

Connecting for Health's Common Framework -- 2006

Do the FIPs Matter?

Concluding remarks on impact of FIPs:

- Setting the stage for effective laws and industry policies.
- The importance of robust standards for meaningful consumer protection.
- However … FIPs are one thing – implementation and enforcement are quite another.

Resources

- Colin Bennett, *Regulating Privacy* (1992)
- Paula Bruening, “Elements of Effective Self-Regulation for Protection of Privacy” at www.ntia.doc.gov (1998)
- Canadian Internet Policy & Public Interest Clinic, *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?* (2006)

Cont’d.

Resources, cont'd.

- Ann Cavoukian, *A Comparison and Gap Analysis of Leading Privacy Codes: An Attempt at Harmonization* (2005)
- Ann Cavoukian, *7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age* (2006)
- Ann Cavoukian and Don Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World* (1997)

Cont'd.

Resources, cont'd.

- Electronic Privacy Information Center & Privacy International, "Transborder Data Flows and Data Havens,", *Privacy & Human Rights* (2004)
- David Flaherty, *Protecting Privacy in Surveillance Societies* (1989)
- Robert Gellman, "Fair Information Practices," in *Encyclopedia of Privacy* (2007)

Cont'd.

Resources, cont'd.

- Paul Schwartz & Joel Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (1996)
- H. Jeff Smith, *Managing Privacy: Information Technology and Corporate America* (1994)
- Robert Ellis Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet* (2004)
- Robert Ellis Smith, *Law of Privacy in a Nutshell* (1993)

Cont'd.

Resources, cont'd.

- Doreen Starke-Meyerring, "European Data Protection Directive," in *Encyclopedia of Privacy* (2007)
- Peter Swire, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (1998)
- U.S. Dept. of Health, Education and Welfare, *Records, Computers and the Rights of Citizens: Report of Secretary's Advisory Committee on Automated Personal Data Systems* (1973)

Contact Information

Beth Givens, Director
Privacy Rights Clearinghouse
3100 - 5th Ave., Suite B
San Diego, Ca. 92103

Phone: (619) 298-3396
E-mail bgivens at privacyrights.org
Web: www.privacyrights.org