

REGULATING PRIVACY IN THE INTERNET AGE

Barry J. Hurewitz

Hale and Dorr LLP

Washington, DC

March 14, 2000

HALE AND DORR LLP

Privacy:

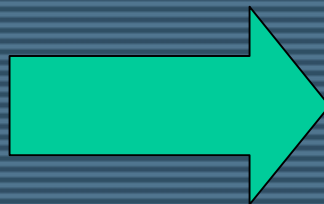
“The right to be left alone -- the most comprehensive of rights, and the right most valued by a free people.”

Justice Louis Brandeis

Olmstead v. United States (1928)

The Internet Changes Everything...

Collection
Processing
Publishing



- Instantaneous
- Automatic
- Inexpensive
- Worldwide
- Linkable

Public Opinion

- Privacy is the #1 Internet issue for consumers
 - *Business Week* survey, 1998
- 87% concerned about online privacy
 - AT&T survey, 1999

State of Confusion?

Consumer Demands

Privacy Laws

Privacy Regulations

“Self-regulation”

Foreign Practices

**Fair
Information
Practices**

Fair Information Practices



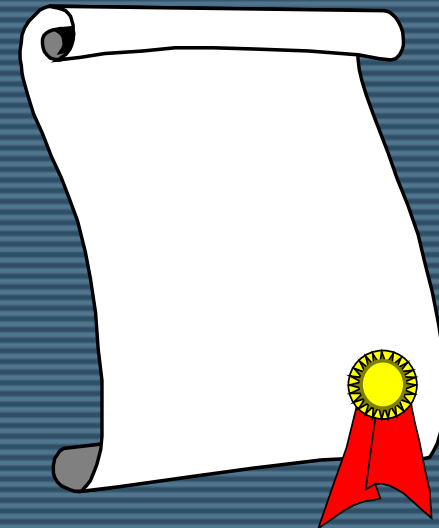
- 1. Notice**
- 2. Choice**
- 3. Access**
- 4. Security**
- 5. Enforcement**

Fair Information Practices

1. NOTICE

Before collection, use, or disclosure,

- Who is collecting data?
- What data is collected?
- How data is collected?
- Why data is collected? (primary uses)
- What other uses? (secondary uses)
- How data is protected?
- What choices are available?



Fair Information Practices

2. CHOICE

Consent to secondary uses of data:



Opt-in

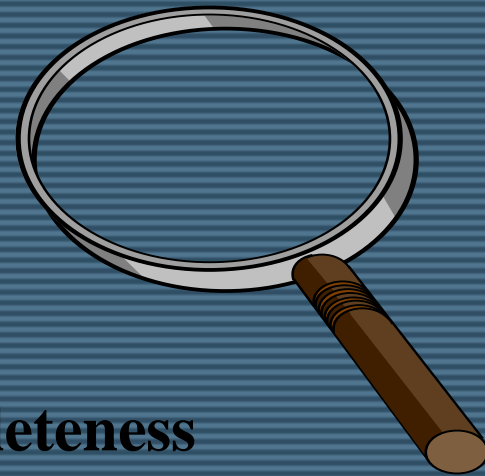
Opt-out

Customization

Fair Information Practices

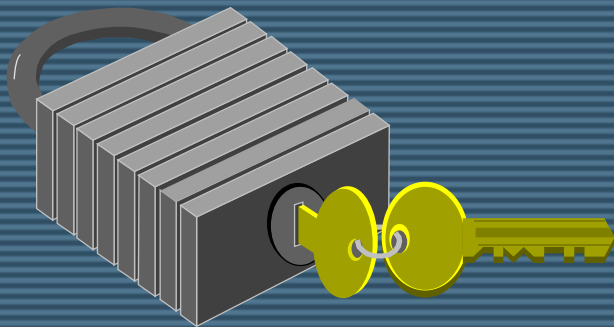
3. ACCESS

- Right to **view** data about oneself
- Right to contest **accuracy & completeness**
- **Procedures** for viewing & requesting revisions



Fair Information Practices

4. SECURITY



- **Data Integrity**

 - Trusted sources

 - Up-to-date

 - De-identification

- **Data Security**

 - Managerial safeguards

 - Technical safeguards

 - Physical safeguards

Fair Information Practices

5. ENFORCEMENT

- Complaint procedure
- Investigation
- Redress
- Sanctions

Federal Internet Privacy Mandates

Internet privacy mandates follow a “**sectoral**” approach:

- **Children’s privacy**
- **Health data privacy**
- **Financial data privacy**

Mandates expand upon Fair Information Practices:

Notice: Timing, placement & content

Choice: Prior consent

Federal Mandates: Children's Privacy

Children's Online Privacy Protection Act

Law enacted 1998

FTC regulations take effect **April 21, 2000**

- Protects **“personal information”**
- Collected by web sites and online services
- From children **under 13**

Focus on

Notice to parents

Advance parental **consent**

Federal Mandates: Children's Privacy

Children's Online Privacy Protection Act

“Personal information”  Identify or contact

Name

Telephone

Physical address

Social Security

E-mail/online contact

“Associated” identifiers

“Sliding scale” of parental consent, based on uses of data

Public disclosure:

“Verifiable parental consent”

Internal use:

E-mail consent + additional steps

Direct replies:

Subsequent notice + opt-out

Protect child:

No consent required

Federal Mandates: Electronic Health Data

- Health insurance reform enacted 1996
- HHS regulations proposed Nov. 1999

Protects **electronic, identifiable health data** handled by:

- Health plans
- Health care providers
- Health care “clearinghouses” (claims processors)
- Business partners

Federal Mandates: Electronic health data

- Defines primary uses of electronic health data:
Treatment
Payment
Health care operations
- **Patient consent** required for secondary uses:
Exceptions include -
Research
Public health
Law enforcement
Emergencies

Federal Mandates: Financial Data

Gramm-Leach-Bliley Act enacted Nov. 1999

FTC regulations proposed March 2000

Comment period ends March 31, 2000

Protects “**nonpublic,**” **personally-identifiable** information

Notice requirements:

Initial notice at start of customer relationship

Annual notices to customers

Notice to consumers prior to disclosure

Choice requirements:

Opt-out of disclosures to nonaffiliated third parties

Federal Mandates: Financial Data

Not Internet-specific, but...

“**Financial institution**” may include anyone “**significantly engaged**” in a “financial activity” with consumers

“**Nonpublic information**” may include names and addresses of customers of “financial institutions”

 Customer lists of B2Cs?

Self-regulation

Sectors without mandatory privacy protections are
“self-regulated”:

e.g., Consumer online privacy

FTC seeks voluntary use of Fair Information Practices
to avoid additional Internet privacy legislation.

“Legislation to address online privacy is not appropriate
at this time.” -- FTC, July 1999

Self-regulation

FTC is watching for voluntary implementation of FIPs:

Websites with posted privacy policies

1998 FTC survey:	2% overall, 44% of busiest websites
1999 Georgetown survey:	44% of sampled websites
1999 OPA survey:	81% of busiest websites
2000 FTC survey:	???

Congress might not wait... current proposals could

Restrict use of “cookies”

Require opt-out of online tracking

Self-regulation: Enforcement

“Self-regulated” DOES NOT MEAN “unregulated”!

FTC can act without new Internet privacy laws:

- **GeoCities** (1998): First net privacy case settled after FTC charged “unfair” and “deceptive” use of online data.

- **ReverseAuction** (2000):

“Self-regulatory efforts by e-businesses to protect their customer’s privacy should be encouraged. But beyond self-regulation, those who violate consumers’ privacy should be promptly called to task.”

FTC action “is an effort to buttress, not supplant or detract from, initiatives of private parties. . . who develop and implement their own privacy arrangements.”

Self-Regulation: Enforcement

Voluntary Privacy Seal Programs

Standard privacy policies

Dispute resolution procedures

Outside monitoring

Referral to law enforcement



Looking Ahead

Pressure to self-regulate

More FTC enforcement

Additional sectoral legislation

Limits on anonymity?

International standards?

Questions?

Barry J. Hurewitz

barry.hurewitz@haldorr.com

(202) 942-8413

HALE AND DORR LLP