WIRELESS PRIVACY:

Legal Considerations for Location-Based Wireless Services

Barry J. Hurewitz
Hale and Dorr LLP
Washington, DC

March 29, 2001

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: Privacy Must Be a Core Element of Any M-Commerce Application

- "Privacy" is consistently rated among the top technology-related concerns among consumers

- 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, 2001

M-COMMERCE PRIVACY RISKS

Different entities present different privacy vulnerabilities

- **CARRIERS**
  - Ownership of data
  - Retention of data
  - Spamming
  - Flowdown safeguards
- **UNAUTHORIZED THIRD PARTIES**
  - Spamming
  - Profiling
  - Stalking
  - Identity Theft
- **AUTHORIZED THIRD PARTIES**
  - Spamming
  - Profiling
  - Physical location tracking
- **GOVERNMENT**
  - Surveillance
  - Discovery

FEDERAL LOCATION TRACKING MANDATES

- Wireless Enhanced 911
  - FCC rules first issued in 1996
  - Phase I: Caller ID & cell site or base station
  - Phase II: Automatic Location Identification (geographic position of caller)

- Communications Assistance for Law Enforcement Act of 1994
  - Telecom carriers required to design networks to enable surveillance
  - FBI & FCC assert that CALEA requires wireless location tracking capabilities as well as numbers dialed
  - D.C. Circuit (2000) limited access to dialed digits and affirmed high legal standard for access to location data

SOURCES OF PRIVACY REGULATION: A State of Confusion

- Mandatory location-based tracking
- Targeted mandatory privacy safeguards
- Industry "self-regulation"
- Inconsistent state laws
- Emerging global standards
- Administrative policies
- Legislative intervention
- Judicial precedents

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

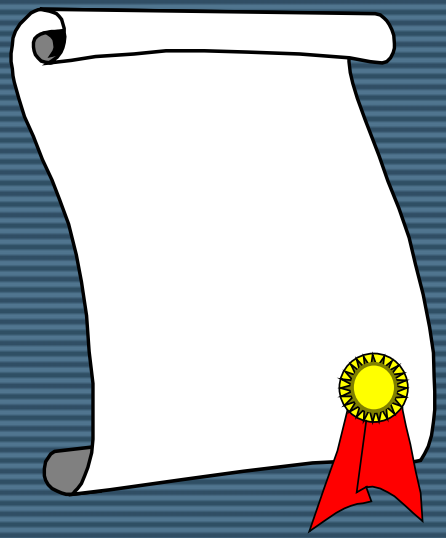
FAIR INFORMATION PRACTICES

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)
- 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

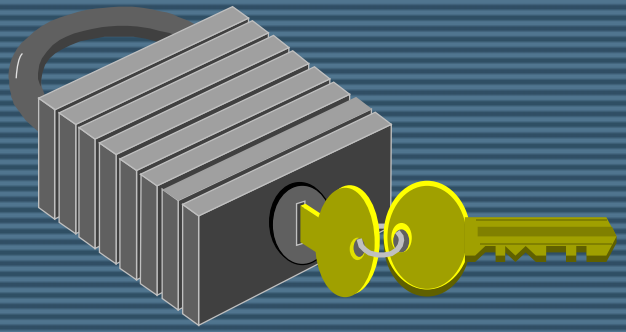
FAIR INFORMATION PRACTICES

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

FEDERALLY-MANDATED SAFEGUARDS: ECPA

- Electronic Communications Privacy Act
  - Prohibits interception of wire, oral, or electronic communications
  - Exception allows access by service providers as necessary to render service
  - Service providers may transmit message contents only to the intended addressee
  - Criminal & private civil liability

FEDERALLY-MANDATED SAFEGUARDS: "Section 222"

- Customer Proprietary Network Information
  - Includes billing info & info about quantity, configuration, type, destination, amount of use
  - Excludes "subscriber list" information
  - Carriers required to protect the confidentiality of individually-identifiable CPNI, subject to customer waiver
  - FCC rules (1998): "Opt-in" consent required to use CPNI for "push" marketing of new services
  - USWest v. FCC (1999): Tenth Circuit rejects FCC rules for restricting commercial speech without sufficient justification of privacy concerns
  - FCC examining alternative approaches

FEDERALLY-MANDATED SAFEGUARDS: Location CPNI

- Wireless Communications & Public Safety Act of 1999
  - Added "location" to CPNI definition
  - "Express prior authorization" to use or disclose
    - Call location information for user of commercial mobile service
    - Automatic crash notification information other than for use in the operation of crash notification system
  - *Exceptions*: 1. emergency dispatch; 2. family notification; 3. other data services to assist in emergency
  - Is mobile web information also protected?

FEDERALLY-MANDATED SAFEGUARDS: Current & Recent Proposals

- Wireless Telephone Spam Protection Act (H.R. 113)
  - Would criminalize unsolicited advertising on mobile telephone messaging system
- Wireless Privacy Protection Act (H.R. 260)
  - Would require written informed consent ("opt-in") for use or disclosure of wireless location
  - Would require carriers to adopt procedures to ensure compliance by third parties
- ECPA 2000 (formerly H.R. 5018)
  - Would have limited use of location information as evidence
- Numerous notice-and-consent bills

FEDERAL ADMINISTRATIVE ACTIVITY

- Federal Communications Commission
  - Revising CPNI privacy rules
  - Interpreting CALEA requirements
- Federal Trade Commission
  - General authority over consumer privacy
  - Dec. 2000 public workshop on wireless consumer issues, including privacy

FOREIGN & STATE STANDARDS

- Foreign laws
  - European Union Directives
    - Data Protection
    - Telecommunications
- State laws
  - Privacy laws vary considerably
  - Several states require consent for vehicle monitoring

INDUSTRY SELF-REGULATION: A Range of Potential Privacy Solutions

- **Device-based solutions**
  - Message traffic encryption (security)
  - User-enabled location data transmission (choice)
  - On-device access control features (security)
  - On-device transmission indicator (notice)

- **Network-based solutions**
  - User-defined permissions (e.g., P3P) (choice)
  - Remote cancel of lost or stolen devices (security)

INDUSTRY SELF-REGULATION: Implementing Fair Information Practices

- Cellular Telecommunications & Internet Association
  - Largest industry group of cellular & PCS carriers
  - Nov. 2000 "Location Privacy Principles"
    - Notice before collecting location data
    - Express (opt-in) consent before collecting location data
    - Secure storage
    - Downstream assurances ("flowdown")
    - Technology neutrality to promote uniform info practices
    - "Safe harbor" protection for adherents to principles
  - Seeking formal adoption by FCC
  - Public comments due April 6, 2001

INDUSTRY SELF-REGULATION: Implementing Fair Information Practices

- Wireless Advertising Association
  - Unit of Internet Advertising Bureau
  - Largest group of wireless advertisers & marketers
  - Nov. 2000 voluntary guidelines for identifiable data
    - Contemporaneous notice via posted privacy policy
    - Description of how location data are used
    - Robust opt-in consent for secondary uses
    - No “spam” (“push” marketing without permission)
    - Data subjects allowed to access, revise & delete
    - Secure storage
  - Comparable to July 2000 Network Advertising Initiative online profiling principles endorsed by FTC

LOOKING AHEAD:
WHAT'S NEXT FOR WIRELESS PRIVACY?

- Increased public concern & awareness
- Proliferation of wireless business models
- Emergence of best privacy practices
- Continued FCC & FTC activity
- Selective enforcement
- Inconsistent international standards
- Privacy litigation
- Possible limits on anonymity
- Targeted legislative intervention

QUESTIONS?

Barry J. Hurewitz

barry.hurewitz@haledorr.com

202-942-8413

www.haledorr.com

www.InternetAlerts.net