International Internet Privacy Issues

Kenneth Slade
Senior Partner, Hale and Dorr LLP

Massachusetts Bar Association
Business Law Section
Health Law Section
April 26, 2001

HALE AND DORR LLP

Overview

- Quick review of current status of U.S. Internet privacy
- European Union's Data Protection Directive
- Canadian legislation
- recent legislation in Latin America
- proposed legislation in Japan

Acknowledgements

- European Union: Thomas Jansen of Linklaters, Oppenhoff & Radler thomas.jansen@linklaters.com
- Canada: Michael Beairsto of Fraser Milner Casgrain LLP michael.beairsto@fmc-law.com
- Latin America: Maria Paula Bonifacini of Allende & Brea mpb@allendebrea.com.ar
- Japan: Takemi Hiramatsu of Asahi Law Offices th@alo.gr.jp

U.S. Perspective

- There is no general privacy legislation in the U.S.
- At a philosophical level, balancing the protection of an individual user's privacy against the incredible value of information about that user, when applied in cyberspace
- At a practical level, companies need to develop an adequate privacy policy and then stick to it
- Manifestations:
  - no longer enough just to have a policy; Federal Trade Commission is looking at how that policy addresses widely-recognized Fair Information Practices:
    - NOTICE about online information collection

U.S. Perspective

- CHOICE regarding uses of that information
- ACCESS to ensure that information is accurate, complete, and up-to-date
- SECURITY and integrity of information collected online; and
- ENFORCEMENT to provide effective recourse for improper breaches of personal privacy.

– Federal Trade Commission will go after you:

- if you do not follow the privacy policy which you have adopted; OR
- if you violate the privacy policy of another web site from which you have "data mined"

EU Data Protection Directive

- Effective on October 15, 1995; had to be transformed into national law by October 15, 1998
- Establishes legal principles for privacy protection and free flow of data within the EU
- Principles are both a minimum and a maximum
- Prohibits the transfer of personal data from EU countries to any countries which do not have "adequate" data protection laws
  - in other words, the United States

EU Rights of the Data Subject

- Right to be informed of the purposes of collection, intended recipients, and data subject's rights, at the time of collection.
- Right to obtain a copy of data about oneself.
- Right to obtain corrections, erasure or blocking of data processed in violation of the Directive.
- Appropriate security safeguards must be adopted by controllers of data.
- Data cannot kept in identified form for longer than necessary for those purposes.

US-EU Safe Harbor Guidelines: Seven Privacy Principles

- NOTICE: state why the information is collected
- CHOICE: individuals must be allowed to opt-out of purposes other than purpose for which data was originally collected
- ONWARD TRANSFER: personal information may be transferred to third party only if such transfer is necessary for the original purpose and the third party agrees to comply with the safe harbor principles
- SECURITY: take reasonable precautions to protect vs. loss, misuse and unauthorized access, disclosure, alteration and destruction

US-EU Safe Harbor Guidelines: Seven Privacy Principles

- DATA INTEGRITY: take reasonable steps to ensure that data is reliable for intended use, accurate, complete and current
- ACCESS: individuals must have access to their data to ensure accuracy
- ENFORCEMENT: opportunity to pursue complaints and disputes
- Companies must provide enforcement mechanisms by:
  - complying with private-sector self-regulatory programs;
  - complying with applicable privacy law or regulation for enforcement; OR
  - committing to cooperate with EU data privacy protection authorities

Status Report on US-EU Safe Harbor

- Final rules published in Federal Register September 19, 2000
- U.S. entities invited to "self-certify" that they would comply with safe harbor principles, subject to enforcement by the FTC
- So far, only about 30 U.S. companies have self-certified

Possible Reasons for Slow Response to US-EU Safe Harbor

- Rely instead on exceptions to EU Directive
  - EU persons may "consent unambiguously" to international data transfers
  - data transfers required to perform a contract
- Perceived lack of immediacy
  - Directive will not be invoked to block transfers until at least June 2001
  - Germany and some other EU countries have not yet enacted legislation
  - BUT France and Sweden have already taken steps to block some transfers

Possible Reasons for Slow Response to US-EU Safe Harbor

- Benefits are not guaranteed
  - some EU data sources may insist upon additional safeguards, such an explicit consent, in order to avoid liability under local data privacy laws
- Possible contractual alternatives
  - EU currently developing model contractual provisions (although adoption has been delayed)
  - by following these models, US companies may avoid subjecting themselves to FTC oversight under the safe harbor program
- Further discussion: February 14, 2001 Internet Alert

Canada's Personal Information Protection and Electronic Documents Act

- Some privacy provisions came into effect on January 1, 2001
  - health information: January 1, 2002
  - all other private sector entities that collect, use or disclose personal information: January 1, 2004
    - unless applicable provincial legislation is enacted by that date
- Federal legislation, but expected to be followed by provincial legislation (already enacted in Quebec; hearings in Ontario; other provinces likely to follow)
  - effort to make Canadian standards consistent with international data protection standards
  - desire to avoid EU countries from blocking data transfers to Canada

Canada's Personal Information Protection and Electronic Documents Act

- Legislation creates a consent-based system which permits individuals to withhold consent in connection with the collection, use or disclosure of their personal information
- Incorporates 10 privacy principles which are based on Canadian Standards Association's Model Code for Protection of Personal Information
  - very similar to US-EU safe harbor principles

Canada's Personal Information Protection and Electronic Documents Act

- Federal statute applies to organizations in respect of personal information that they collect, use or disclose in the course of commercial activity across provincial or international boundaries
- Other provisions apply to employers in federally regulated industries (e.g., telecomm, broadcasting, banking and airlines) which collect personal information on employees
- Further discussion: February 5, 2001 Internet Alert

Scope of Canadian Privacy Legislation

- Covers “personal information” about an identifiable individual, but excludes the name, title or business address or telephone number of an employee of an organization
- Personal information provided by Canadian users and collected by a U.S. company through its web site is probably covered
- BUT enforcement and jurisdiction are separate issues

Two-Step Analysis of Applicability to U.S. Data Collectors

- What is the situs of the personal information collection activity?
  - determination to be made by Canadian Privacy Commissioner
- Is collection in the course of commercial activity?
  - will depend on the purpose of web site (i.e., advertising? selling goods? purely informational?)

Latin American Privacy Overview

- LA countries are enacting privacy legislation for three main reasons:
  - to remedy past privacy violations
  - to promote e-commerce
  - to ensure EU data exchange
- Most LA countries are enacting comprehensive privacy laws for both the public and private sector, in some cases complemented with particular laws for specific types of information
- Right to privacy recognized in most LA constitutions (Argentina, Brazil, Chile, Mexico, Peru, etc.)

Recent and Pending Legislation

- Argentina 1994 Constitution, Habeas Data Bill (enacted November 2000)
- Brazil 1988 Constitution, 1990 Code of Data Consumer Protection and Defense (grants consumers the right to access and correct their personal information), Data Privacy Bill in conformance with OECD guidelines (pending since 1996)
- Chile Constitution, Law of the Protection of Private Life. Chapter on use of financial, commercial and banking data (came into force October 1999)
- Mexico 1917 Constitution, E-Commerce Act (came into force June 2000, amending Consumer Protection Act)
- Peru 1993 Constitution, Data Protection Bill (pending since October 1999)
- Paraguay Data Protection Act (came into force December 28, 2000)

Following the EU Standard

- Most LA privacy laws and bills follow EU Directives very closely
  - rights of data subjects (Argentina, Chile and proposed laws in Brazil and Peru)
  - data processing rules
  - liability and enforcement
  - transfer to other countries (Argentina and proposed Brazilian law)
    - safe harbor rules with the United States may need to be negotiated
- By following the EU standard, there is an expectation that privacy laws will be harmonized between Latin American countries
- Further discussion: December 11, 2000 Internet Alert

Japanese Internet Privacy

- Currently, there is no uniform Japanese law on privacy
- Recognized as a constitutional right under case law
- Public sector:
  - "Act for Protection of Computer Processed Personal Data Held by Administrative Organs" (1988), applied to the administrative organs of the central government
  - "Personal Data Protection Ordinances", promulgated by many local governments
- Private sector:
  - No comprehensive legislation
  - Self-regulation policy

Japanese Internet Policy

- "Guidelines for Protection of Personal Data in Telecommunications Business" (1991), "Guidelines for Protection of Subscribers' Personal Data Regarding Broadcast Viewers" (1996) and "Guidelines for Protection of Communicators' Personal Data in Utilization of Services of Notifying Communicators' Data" (1996), issued by the Ministry of Posts and Telecommunications
- "Guidelines for Protection of Computer Processed Personal Data in Private Sector" (1997), issued by the Ministry of International Trade and Industry

- first systematic survey of consumer privacy was not organized until 1999
- general view that national legislation is needed
  - for uniformity
  - to cover private collection of data
  - for sake of complying with international standards (i.e., EU Data Protection Directive)

Proposed Japanese Act for Protection of Personal Data

- Approved by Japanese Cabinet March 27, 2001
- Expected to be in force from April 2003
- Clarifies basic principles for both private and public sectors
- Provides for various responsibilities generally applicable to all “personal data handling entrepreneurs”

Japanese Legislation: Basic Principles for Handing Personal Data

- information should be used for specific purposes, and only to the extent necessary (consent)
- information should be obtained by proper methods (notice)
- information's accuracy should be maintained (data integrity)

Japanese Legislation: Basic Principles for Handing Personal Data

- information should be used only after appropriate safeguards are in place (data security)
- individuals whose information is collected should be able to demand correction or deletion of personal details (access)

Proposed Japanese Legislation

- Includes criminal penalties
- Exemptions proposed for news media, academic research, and religious and political activities
- Not yet clear whether or not the Japanese legislation would be deemed adequate under the EU Data Protection Directive

Conclusion

- The number of jurisdictions with formal privacy laws is expanding rapidly.
- There is no single privacy standard being adopted in those jurisdictions.
- Compliance with the toughest standard (i.e., European Union) does seem to satisfy substantive requirements of the less demanding jurisdictions.
- Even if EU standard is followed, there may still be registration and record-keeping requirements in other jurisdictions.

For Further Information

- Subscribe to Hale and Dorr Internet Alerts at www.haledorr.com/practices/email_alerts.asp?areaID=17
- Contact Ken Slade
  - kenneth.slade@haledorr.com
  - telephone: 617-526-6184
  - fax: 617-526-5000
  - mailing address:
    - 60 State Street
    - Boston, Massachusetts 02109