Morris, Manning & Martin, LLP

Media Room

- Events Calendar (/media-room/events-calendar)
- Events (/media-room/events-and-webinars)
- News (/media-room/news)
- Client Alerts (/media-room/client-alerts)
- Publications (/media-room/publications)

Privacy & Data-Mining On The Internet

Share:

Author(s)

- John C. Yates (http://www.mmmlaw.com/our-people/employee-directory/attorneys/john-c.-yates)

Practice Areas

- Technology (http://www.mmmlaw.com/practice-areas/technology)

Industries

- Technology (http://www.mmmlaw.com/industries/technology)

I. Introduction

A. Overview

Internet data collection and data-mining present exciting business opportunities. However, potentially large changes in European privacy laws, as well as contemplated changes in American laws, suggest that lawyers approach these issues with both careful planning and caution.

This article will review --

- The Current State of United States Data Privacy Law
- The European Union Personal Data Directive
- Recent United States Legislative Proposals
- Clinton Administration Approaches to Data Privacy
- Practical Considerations Given the Potential Legal Changes in Data Privacy Laws

B. Recent Privacy Concerns

American Express: American Express recently announced a collaboration with Knowledge Base Marketing, Inc. Knowledge Base possesses records of 175 million Americans, which it will combine with records of consumer purchases from American Express. This compilation will then be used to help companies conduct targeted marketing campaigns. American Express is not planning to specifically notify its cardholders about this

operation.

P-TRAK: In 1996, concern was expressed about a vendor making social security numbers and other personal information available to its customers through its database. The vendor ultimately ceased making social security numbers availability.

Cookies: Cookies are small data files sent by Web sites to the hard drives of computers which are used to visit the Web site. These data files are individually distinct and allow the Web site to track each particular visitor to a Web site. Cookies raise privacy concerns because they allow Web site operators to keep records of what a Web site visitor does at the site, who the visitors are and where they can be reached by the Web site operator.

II. The Current State of United States Data Privacy Law

There is no overall privacy statute that generally governs the use of commercial database information in the United States. Several other laws are potentially relevant to this issue, however.

A. Electronic Communications Privacy Act (18 U.S.C. § 2701-2704, 2707)

Places limitations on monitoring information flowing through the Internet and online systems.

Protects email from disclosure or use of the message contents by anyone except the intended recipient.

B. Federal Trade Commission Act (15 U.S.C. § 41)

§5(a) of the FTC Act (15 U.S.C. § 45(a)(1)) makes it unlawful for one to engage in "unfair or deceptive acts or practices in or affecting commerce."

On December 11, 1997, an FTC official stated that companies which falsely claim to be adhering to privacy policies may be in violation of the FTC Act. Those companies may be sued by the FTC as a result.

C. Privacy Torts

In the United States, it is conceivable that an individual could rely on a common law state privacy tort to enforce a claim of a privacy violation.

1. Intrusion Upon Seclusion: This tort requires the following elements to be demonstrated:

- Intention or knowledge
- Reasonable expectation of privacy

The principal issue is whether there is a reasonable expectation of privacy on the Internet. Although there is no authority on this issue to date, numerous polls have been taken which reflect that people fear they have no privacy on the Internet.

2. Public Disclosure of Private Facts: This tort requires the following elements to be demonstrated:

- Publicity of the information to the "public at large"
- The defendant must have caused the disclosure
- The facts must have initially been private
- The disclosure must be "highly offensive to a reasonable person."

3. Misappropriation

This tort involves using another person's name for an advantage, without that person's consent. Many states have adopted statutes which govern misappropriation, with the intent to protect the use of celebrity names. However, the language in these statutes may be sufficiently broad to support a claim based on the commercial use of ordinary personal information.

4. Stern v. Delphi Internet Services Corp.

(N.Y. Sup. Ct. 1995): Howard Stern, the radio celebrity, sued Delphi, an ISP, over the use of his picture on one of their electronic bulletin boards. Stern sued under a New York privacy statute. The court held that Delphi was not liable because its use was an incidental use, an exception to the statute. The court observed that Delphi's use was similar to that of a news vendor and protected its use accordingly.

D. Self-Regulation

Many trade associations have privacy principles and guidelines which govern how their members do business. Here are two examples:

1. The Direct Marketing Association (http://www.the-dma.org) (See Attachment 1)

The Direct Marketing Association (DMA) has more than 3,600 members in 50 countries. It has promulgated general guidelines for protecting personal data, as well as specific principles for electronic commerce. DMA has recently decided to require that all its members abide by these ethical guidelines or they will be expelled from DMA. This requirement will begin in July 1999.

a. Guidelines for Personal Information Protection
   (1) Personal data should be collected by fair and lawful means for a direct marketing purpose.
   (2) Direct marketers should limit the collection of data to only that deemed necessary for direct marketing.
   (3) The data should be accurate and complete and should be kept no longer than necessary.
   (4) Individuals can request personal data about themselves, as well as challenge the accuracy of the personal data.
   (5) Consumers who provide data that may be rented or sold should be told of that potential and given an opportunity to delete their data.
   (6) The collection, rental, sale and use of consumer data should be constrained to direct marketing purposes.
   (7) Each direct marketer is responsible for the security of their data.
   (8) Visitors to personal data processing and storage sites should only be allowed to visit if they have the express permission of the direct marketer and are accompanied by an employee at all times.
   (9) When transferring data between direct marketers, the receiver is responsible for the security of the data during the transfer.<,/li>
   (10) An ethics committee of the DMA has jurisdiction to review individual complaints in violation of these Guidelines.

b. DMA's Marketing Online Privacy Principles and Guidance
   (1) Online Notice: Direct marketers should prominently display a notice that indicates who they are, what information they are collecting, the purposes of collecting the information, the types of people who will receive the information and the method by which one can limit the disclosure of

information.
(2) Opting Out: Marketers should inform customers of their opt-out choices and act upon the wishes of the consumers.
(3) Unsolicited Email: These messages should be clearly marked as solicitations and identify the marketer. Marketers should also provide recipients with a method of preventing future messages from being sent to those recipients.
(4) Online Data Collection Involving Children: Marketers should take into account their audience when deciding whether to collect data. Marketers should encourage parents to monitor their children while their children are online. Use of collected data should be limited to marketing purposes.

2. TRUSTe (http://www.truste.org)

a. TRUSTe is an initiative that seeks for Web sites to utilize the "trustmark," a symbol that indicates the Web site complies with TRUSTe privacy disclosure requirements.
b. Trustmark recipients must have a privacy statement which discloses at a minimum:
    - What type of data is gathered
    - How the data will be used
    - Who will receive the data.

    Recipients must display the trustmark and adhere to its privacy statement.
c. TRUSTe will periodically audit its licensee sites to ensure they conform with TRUSTe standards. Conformance reviews will also occur by Coopers & Lybrand and KPMG Peat Marwick.
d. TRUSTe is supported by various companies, including AT&T, Excite, IBM, Land's End, Netcom, Netscape and Oracle.

3. Privacy Policies

(See Attachment 2)

III. The European Union Personal Data Directive (1995 O.J. (L. 281) 31)

(See Attachment 3)

Full Title: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The Directive must be adopted by each of the 15 members of the European Union by October 24, 1998. (Article 32)

A. Key Provisions of the Directive for European Actors

1. Scope

(Articles 2, 3)

Personal data is broadly defined to include any information relating to an identified or identifiable natural person.

Processing of personal data is also broadly defined. It means any operation or set of operations which is performed upon personal data, whether or not by automatic means.

The Directive applies to the processing of personal data which occurs at least partly by automatic means or to processing which either forms part of a filing system or is intended to form part of a filing system.

Exception The Directive does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

2. Data Quality

(Article 6) Personal data collected must be --

- Processed fairly and lawfully
- Collected for specified, explicit and legitimate purposes without further processing incompatible with those purposes
- Adequate, relevant and not excessive in relation to the purposes of collection or processing
- Accurate and kept up to date where necessary
- Kept no longer than necessary in a form which identifies the data subjects.

3. Legitimacy of Data Processing

(Article 7) Personal information may only be processed if --

- The data subject unambiguously provides consent or
- Processing is necessary for a contract of which the data subject is a party or
- Processing is necessary to comply with a legal obligation of the data subject or the data controller or
- Processing is necessary for a task carried out in the public interest.

4. Special Categories of Data

(Article 8) The Directive has special treatment for personal information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership and data involving health or sex life.

5. Data Controller Identification

(Articles 10, 11) The data subject must be provided with the identity of the data controller, the purposes of the data processing and any other information that is necessary to ensure that personal information is processed in a fair and lawful manner.

6. Access Rights

(Article 12) Every data subject shall have the right to obtain the following information from the controller:

- Confirmation as to whether the data relating to the subject is being processed
- The purpose of the processing
- The categories of data being processed
- The recipients or categories of recipients who will receive the data.

Additionally, the data subject has, where appropriate, the right against the data controller to rectify, erase or

block data processing which does not comply with the Directive, if the data is incomplete or inaccurate.

7. Objection Rights

(Article 14) A data subject has the right to object to personal information processing for direct marketing or other purposes.

8. Automated Processing Opt-out Provision

(Article 15) A data subject has the right not to be subject to a decision based solely on automated data processing, which is intended to evaluate personal aspects of the data subject, such as creditworthiness, and will have legal or otherwise significant effects on the subject. This right is subject to contracts the subject may have entered into as well as satisfaction by the Member State that suitable safeguards protect the subject's interests.

9. Remedies

(Articles 22, 23, 24) Individuals may seek recourse under their respective national laws. Data subjects are entitled to receive compensation for damages from the appropriate data controller, if the controller was responsible for the damages.

B. Implications for Non-European Actors

1. European Member States may only allow for the transfer of personal data to other countries if that other country ensures an "adequate level of protection." (Article 25)

2. Article 25 notes further that an adequate level of protection is to be assessed in light of all the circumstances surrounding a data transfer operation, particularly focusing on:

- The nature of the data
- The purpose and duration of the proposed processing operation
- The country of origin
- The country of final destination
- The rules of law in the other country
- The professional rules and security in the other country.

3. The Member States are to inform each other of countries that do not provide an adequate level of protection. They are also to take appropriate measures to prevent the transfer of data to those countries which do not meet their requirements.

4. To aid in defining "adequate protection," the European Commission's Working Party on the Protection of Individuals with Regard to the Processing of Personal Data released a paper, entitled First Orientations on Transfers of Personal Data to Third Countries -- Possible Ways Forward in Assessing Adequacy.

a. This Paper contemplates the creation of White Lists of nations which possess adequate data protection.
b. For those nations not on the White Lists, the Paper sets forth a category of transfers that would be particularly sensitive and more likely to be carefully examined:
    - Transfers of sensitive information described in Article 8 of the Directive
    - Transfers which carry the risk of financial loss (such as credit card payments over the Internet)
    - Transfers carrying a risk to personal safety
    - Transfers made for the purpose of making a decision which significantly affects an individual (such

as whether to grant credit)
    - Repetitive transfers involving massive volumes of data
    - Transfers involving the collection of data in a covert or clandestine manner (such as Internet cookies).

c. In defining "adequate protection," the Working Party noted the two key elements are the content of the equivalent rules and the means by which those rules are enforced. The Working Party provided a list of 6 principles which should be reflected in the content of the other country's rules, at a minimum:

    (1) Purpose Limitation. Data should only be processed for a specific purpose.
    (2) Data Quality and Proportionality. Data should be accurate and not excessive in relation to the purpose of its acquisition.
    (3) Transparency. Subjects should be informed of the identity of the data controller and the purpose of the processing.
    (4) Security. The data controller should take appropriate technical and organizational security measures.
    (5) Rights of Access, Rectification and Opposition. The data subject should have the right to obtain the data obtained by the controller, the right to clarify inaccuracies and the right to oppose certain uses of the data.
    (6) Restrictions on onward transfers to other countries. Further transfers should only be allowed if the next country also has an adequate level of protection.

    - (1) Sensitive Data. Additional safeguards should protect sensitive data of the kind listed in Article 8.
    - (2) Direct Marketing. Data subjects should be able to opt-out of the use of their data for direct marketing purposes.
    - (3) Automated Individual Decisions. Data subjects should have safeguards when the data is to be used in automated individual decisions.

    In addition, the following 3 principles were offered for their use when they apply:

d. Aside from the issue of the content of the rules, the Working Party observed that to effectively enforce the rules, a system must (1) ensure a good level of compliance, (2) support and help individual data subjects to enforce their rights and (3) provide appropriate redress when the rules are violated.

5. Potential Safe Harbors

(Article 26) The Directive allows for data transfers to occur involving other countries without an adequate level of protection under the following circumstances, including:

- Where the data subject has given his unambiguous consent to the proposed transfer
- Where the transfer is necessary for the performance of a contract between the data subject and the data controller
- Where the transfer is necessary for the performance of a contract which benefits the interests of the data subject, but is between the data controller and a third party.

6. A Less Reliable Safe Harbor

The Working Party paper cautions against reliance upon another safe harbor, in Article 26(2). This provision allows for a transfer where the other country does not provide an adequate level of protection, if the data controller finds adequate safeguards in the appropriate contractual clauses.

The reasons for their cautions are these:

1. Article 26(2) still requires adequate safeguards, even in the contractual provisions.

2. Article 26(2) is further modified by Article 26(3). Article 26(3) places the burden on a Member State to inform the rest of the European Union about any authorizations granted under 26(2). This is a reversal of the Directive's other provisions, which only require an equivalent disclosure when adequate protection has not been granted by a Member State, under Article 25.

IV. Recent United States Legislative Proposals

A. Data Privacy

1. Government Data

a. Federal Internet Privacy Protection Act of 1997 (H.R. 1367)

Summary: Prohibits Federal agencies from making available through the Internet certain confidential records with respect to individuals and to provide for remedies in cases in which such records are made available through the Internet.

Status: Referred to the House Government Reform and Oversight Committee, April 17, 1997.

Sponsor: Rep. Mark Barrett (D-WI)

b. Social Security Information Safeguards Act of 1997 (H.R. 1331)

Summary: Requires the Commissioner of Social Security to assemble a Social Security Information Safeguards Panel to assist the Commissioner in developing appropriate mechanisms and safeguards to ensure the confidentiality and integrity of personal Social Security records made accessible to the public.

Status: Referred to the House Ways and Means Committee, April 15, 1997.

Sponsor: Rep. Barbara Kennelly (D-CT)

2. Commercial Data

a. Children's Privacy Protection and Parental Empowerment Act of 1997 (H.R. 1972)

Summary:

(1) Any seller of data who is found to knowingly purchase or sell data containing the personal information (such as name, telephone number, social security number or email address) of a child who is under 16 years of age may be fined or imprisoned unless that seller receives the written consent of the child's parent. The data vendor must also comply with requests from parents about (1) the source of the personal information, (2) the contents of the information about the parent's child and (3) the identity of the purchasing parties.

(2) Anyone who uses any personal information about a child of under 16 years of age to contact that child in order to sell goods or services to the child or a parent may be fined up to $5,000 if that person fails to comply with requests from parents about (1) the source of the personal information, (2) the contents of the information about the parent's child, (3) the identity of the purchasing parties and (4) discontinues

providing that personal information about the parent's child to third parties.

(3) Anyone who uses prison labor to process data or distributes or solicits personal information about a children of less than 16 years of age with the intent to abuse, cause physical harm or sexually exploit the child, shall be fined or imprisoned.

Status: Referred to House Subcommittee on Crime (via Committee on the Judiciary), June 25, 1997. Subcommittee hearings held, April 30, 1998.

Sponsor: Bob Franks (R-NJ)

b. Communications Privacy and Consumer Empowerment Act (H.R. 1964)

Summary:

(1) Empowers the Federal Trade Commission to commence a proceeding six months after the Bill has been enacted to investigate whether consumers can determine (1) whether information is being collected about them, (2) whether that information is being used for purposes unrelated to the original collection and (3) the exercise of control over the collection of personal information. The FTC will propose changes in FTC regulations consistent with those three objectives and complete those changes within one year of the Bill's enactment.

(2) Empowers the Federal Communications Commission to investigate the impact of interconnected communications networks, such as telephone, cable, and satellite, on those three objectives. The FCC is to propose changes in their regulations consistent with the three objectives and complete those changes within one year of the Bill's enactment.

(3) Amends the Communications Decency Act to add a provision which requires Internet Service Providers to provide screening software which limits Internet access to material that is inappropriate for children.

Status: Referred to the House Subcommittee on Telecommunications, Trade and Consumer Protection (via the House Commerce Committee), June 26, 1997.

c. Consumer Internet Privacy Protection Act of 1997 (H.R. 98)
(See Attachment 4)

Summary: Unlike current privacy protections, which allow individuals to opt-out, this Bill only allows information to be used by Internet Service Providers if individuals opt-in to the database.

Interactive computer services, which are defined as those services that provide multiple users with computer access to Internet, cannot disclose any "personally identifiable information" without the consent of the individual service subscriber.

The Bill also requires interactive computer services to reveal the identity of third party recipients of personally identifiable information to the relevant service subscriber.

The Federal Trade Commission is empowered by the Bill to enforce its provisions.

Status: Referred to the House Commerce Committee, January 7, 1997

Sponsor: Rep. Vento (D-MN)

d. Data Privacy Act of 1997 (H.R. 2368)
See Attachment 5)

Summary

(1) Establishes a computer interactive services industry working group to establish voluntary guidelines: (1) limiting the collection of personal information for commercial purposes obtained through any interactive computer service; (2) relating to the distribution of unsolicited commercial email messages; (3) and to provide incentives to follow the guidelines, including icons which indicate guideline adherence.

(2) The Bill also prohibits the use of personal information for commercial marketing purposes, the use of personal health or medical information for medical purposes, or the display of another person's social security number through an interactive computer service, unless that person had a prior business relationship or valid contract with the information provider.

Status: Referred to the House Commerce Committee, July 31, 1997

Sponsor: Rep. Billy Tauzin (R-LA)

e. Social Security On-Line Privacy Protection Act of 1996 [sic] (H.R. 1287)

Summary: Prohibits interactive computer services from disclosing an individual's social security numbers or related personal information without his or her prior, informed, written consent. Individuals are allowed to revoke their consent at any time, upon which the interactive computer service will cease disclosing the private information.

Status: Referred to the House Commerce Committee, April 10, 1997

Sponsor: Rep. Robert Franks (R-NJ)

B. Unsolicited Email / "Spam" Regulation

1. Electronic Mailbox Protection Act of 1997 (S. 875)

Summary: A person is subject to a penalty of up to $5,000 if they do one of the following:

(1) Sends unsolicited email from an unregistered or fictitious address to prevent responses to the message.
(2) Disguises the source of the unsolicited email message to prevent recipients from using a mail filter.
(3) After sending an unsolicited email message, fails to comply with a request to terminate sending further messages.
(4) Distributes a collection of email addresses while knowing that some of the recipients do not want to receive unsolicited email.
(5) Initiates an unsolicited email message despite prior notice that the recipient does not want to receive

an unsolicited message.
(6) Registers or creates an Internet domain name for the principal purpose of initiating the transmission of unsolicited email.
(7) Sends an unsolicited email message through an interactive computer service knowing that sending that message violates the rules of the interactive computer service.
(8) Despite the contrary rules of an interactive computer service, accesses that service's server to collect email addresses.
(9) Initiates the transmission of bulk unsolicited email messages but then splits up the messages to circumvent this Bill.

Status: Referred to the Senate Commerce, Science and Transportation Committee, June 11, 1997.

Sponsor: Robert Torricelli (D-NJ)

2. Netizens Protection Act of 1997 (H.R. 1748)

Summary: Amends the 1934 Communications Act to --

(1) Ban the transmission of unsolicited advertisements by electronic mail when there is no preexisting and ongoing business or personal relationship, unless the recipient provides an express invitation to send such advertisements.
(2) Require unsolicited advertisements begin with the date and time the message is sent, the sender's identity and the sender's return email address.

Status: Referred to the House Commerce Committee, May 22, 1997

Sponsor: Chris Smith (R-NJ)

3. Unsolicited Commercial Electronic Mail Choice Act of 1997 (S. 771)

Summary:

(1) Requires any person transmitting an unsolicited commercial electronic mail message to include as part of the message the word "advertisement" at the beginning of the message, as well as the name and address of the sender.
(2) Empowers the Federal Trade Commission with authority over unsolicited electronic mail. This includes the ability to conduct investigations and impose fines.
(3) Allows a state to bring an action on behalf of its residents, so long as that state notifies the Federal Trade Commission.
(4) Requires that senders of unsolicited electronic mail terminate those messages upon the request of the recipients of those messages.

Status: Referred to the Senate Commerce, Science and Transportation Committee, May 21, 1997.

Sponsor: Frank Murkowski (R-AK)

V. Clinton Administration Approaches to Data Privacy

A. New Comprehensive Privacy Action Plan

(See Attachment 5)

Announced May 14, 1998 by Vice President Gore, the Plan consists of the following elements:

- Medical Privacy: The Vice President called on Congress to pass legislation which would restrict access to medical records and allow for individuals to correct their records.
- One Stop Opt-Out: The Vice President indicated that the FTC will be sponsoring a new Web site, located at "www.consumer.gov". At this site, consumers will be able to (1) bar companies from pre-screening their credit records, (2) restrict the sale of their drivers' license data to data vendors and (3) remove their names and addresses from direct-mailing lists.
- Appropriate Use of Federal Government Data: The Vice President announced that the President had sent a new Memorandum to agency heads to ensure that new technologies are used in accordance with existing governmental privacy laws and to evaluate legislative proposals with regards to those governmental privacy laws.
- Privacy Summit: The Vice President asked the Commerce Department to hold a summit within the month of June to bring together privacy advocates and industry representatives. This summit will focus on self-regulation and children's privacy issues.

B. A Framework for Global Electronic Commerce

Announced July 1, 1997 by President Clinton, the Framework is the equivalent of a Clinton Administration Mission Statement regarding electronic commerce. It is based upon these five principles:

1. The private sector should lead.
2. Governments should avoid undue restrictions on electronic commerce.
3. Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.
4. Governments should recognize the unique qualities of the Internet.
5. Electronic Commerce over the Internet should be facilitated on a global basis.

Regarding privacy issues, the Framework endorses self-regulatory regimes. The Administration indicated that it would engage its key trade partners, such as the European Union, to increase understanding of the American market-driven approach to privacy. Although the Framework endorses industry self-regulation, it concludes that if effective protection is not possible through this method, the Administration will reevaluate its approach.

By July 1, 1998, a privacy self-regulation progress report is due before President Clinton and Congress, to evaluate the effectiveness of self-regulation.

C. Department of Commerce: Elements of Effective Self-Regulation for Protection of Privacy

In support of President Clinton's Framework, the Department of Commerce has published a discussion draft of a staff discussion paper on privacy self-regulation. This paper identifies the key principles that are necessary for an effective self-regulatory regime.

1. Principles of Fair Information Practices

a. Awareness: Consumers need to know --
    - The identity of the collector of their personal information

- The intended uses of the information
- The means by which they may limit its disclosure.

Data vendors are responsible for raising consumer awareness about these issues and can do so through:

- Privacy Policies
- Notification
- Consumer Education

b. Choice: Consumers must be able to make choices about whether and how their information will be used. To make these choices possible, consumers must be offered simple, easily understood and affordable mechanisms. In some circumstances, such as medical information or children's information, data vendors should not use the data without the consent of the appropriate person.
c. Data Security: Companies should take reasonable precautions to protect the data's accuracy and integrity. This should extend to those third parties to whom they may send data.
d. Consumer Access: Consumers should be able to access the information that has been collected about them, as well as be able to correct any inaccuracies.

2. Enforcement

a. Consumer Recourse: Companies should offer some form of dispute resolution to provide redress for consumer complaints.
b. Verification: Companies must be able to demonstrate that the claims they make about their privacy protection regimes are accurate.
c. Consequences: Examples of consequences include cancellation of the right to use a seal or logo, posting the name of the violator on a bad actor list or disqualification from a trade association. FTC liability may also exist if the company has failed to live up to its privacy policy.

D. Federal Trade Commission

1. Monitoring Self-Regulation

(See Attachment 7)

In March 1998, the FTC conducted a survey of commercial Web sites to determine the extent to which they disclose their privacy policies and whether consumers are offered a choice as to the online collection and use of their personal data.

The FTC surveyed 1200 Web Sites, included the 100 most frequently visited sites, 200 children's sites and 900 commercial sites from a database of sites maintained by Dun & Bradstreet.

The FTC looked for 4 elements in privacy policies, aside from whether they are easy to find:

1. *Notice to consumers as to whether their information will be transferred to other parties*
2. *Whether a choice is provided to consumers as to the use of the data*
3. *Whether consumers can access their own personal data*
4. *Whether consumers are informed about security precautions taken to protect the data.*

The results of this FTC study will be included in an upcoming report to Congress, which will focus on the

effectiveness of self-regulation for personal data. This report will be published in June 1998.

2. Individual Reference Services

a. In December 1997, the FTC published a report to Congress approving the self-regulation principles promulgated by the Individual Reference Services Group (IRSG).
b. Individual reference services are vendors who collect and disseminate personal identification information about consumers, such as their credit ratings.
c. The IRSG comprises 14 companies, a substantial majority of the companies comprising the individual reference service industry.
d. The IRSG Principles are as follows:

(1) Restrictions on the Availability of Non-Public Information: The IRSG treats customers differently, based on their access to non-public information. The greater the information access of the customer, the greater the controls on the customer.
(2) Monitoring Use and Maintaining Audit Trails: Each service is required to maintain a record of higher-end subscribers, such as professional users. This record must contain the solicitor's identity, the types of uses the subscriber employed and the terms and conditions that the subscriber agreed to. This record is to be kept for three years after the service-subscriber relationship ends. Services do not have to record what information their subscribers' accessed.
(3) Consumers' Access to Personal Information and Methods to Ensure Information Accuracy: The methods to ensure accuracy include only accepting data from reputable sources and correcting inaccuracies presented by individuals. Alternatively, an IRSG member can direct the individual to the source of the data.
(4) Ability to Opt-Out: Individuals may opt-out of the general distribution of their information, but cannot opt-out of distribution to professional and commercial users.
(5) Consumer Education and Openness: The services are to educate the public and users about privacy concerns. Each service must have a privacy policy statement which meets requirements such as disclosing to whom it may disclose information. Services are to also notify consumers through advertisements or other educational efforts.
(6) Compliance Assurance: IRSG members' practices are subject to review by a reasonably qualified independent professional service.

e. The FTC did criticize the IRSG Principles

(1) The IRSG Principles fail to limit or control the use of publicly available information.
(2) The Principles fail to require specific audit trails of the records accessed by each user.
(3) The Principles fail to allow individuals to access public records or publicly available information maintained by IRSG members.

Despite these concerns, the FTC has recommended that the IRSG Group be allowed to demonstrate that their Principles are a viable self-regulatory system. In addition, IRSG members have agreed to re-examine the FTC's concerns by June 1999.

3. Unsolicited Email (Spam)

The FTC has engaged in three initiatives in this area:

- Self-Regulation: A group of interested parties, led by the Center for Democracy and Technology, is preparing a report outlining potential options on this front.
- Enforcement Actions: The FTC has brought several actions against individuals that it believes are making fraudulent solicitations through unsolicited commercial email, including FTC v. Maher (D. Md., filed Feb. 19, 1998) and FTC v. Cooley (D. Ariz. filed Mar. 4, 1998).
- Education: FTC staff has produced materials warning consumers about the dangers of unsolicited commercial email.

E. Medical Information Privacy & the Department of Health & Human Services

Pursuant to the 1996 Health Insurance Portability and Accountability Act, the Department of Health and Human Services must promulgate regulations for medical information privacy standards within six months of August 1999, if Congress has failed to enact health privacy legislation by August 1999.

The Secretary of Health and Human Services has recommended that five principles guide any proposed legislation:

1. Restricted Purposes: Health care information should be only disclosed for health care purposes.
2. Security: Those who legally receive health information must take reasonable precautions to protect the information.
3. Consumer Control: Individuals should have the ability to know what is in their records, who has examined their records, how they can change inaccurate information in their records and where they can obtain their records.
4. Accountability: To enforce these principles, those found violating them should be severely punished, including the possibility of criminal penalties.
5. Balancing Of Interests: Privacy interests should be balanced with other national priorities.

VI. Practical Considerations Given the Potential Legal Changes in Data Privacy Laws

A. Monitor Developments

Follow the issue closely during 1998. U.S. law could change rapidly in response to negotiations with the European Union over its Personal Data Directive.

B. Review Directive Implementation

Carefully follow the development of the Directive and consider its implications upon your operation. The scope of the Directive may even be broad enough to include email messages which contain personal data. Each Member State of the European Union must adopt the Directive, but they may legislate slight changes from the Directive when it is adopted.

C. Assess Web Sites

Determine whether your Web site can differentiate users based on geographic location. This may be necessary if you anticipate problems complying with the Directive.

D. Review Data Collection

Investigate how your Web site collects information. Is it automatic collection, via a cookie, or voluntary

information? The European Union may react strongly against the automatic collection of data when that data is collected without the knowledge of the data subjects.

E. Review Users of Data

Determine how the data from your Web site will be used. If you are seeking the consent of your customers to use their data, it is particularly important that you establish all of the specific uses before obtaining their consent. Under the Directive, the purposes of data collection have to be both specific and explicit.

F. Adopt Privacy Policies

(See Attachment 2)

Consider including a prominent privacy policy statement on your Web site. It should include treatment of the following issues:

- Your identity (the data controller)
- The purposes for collecting data
- How long the data will be kept
- How the data is kept secure
- The procedures for keeping the data accurate, including how individuals can correct inaccuracies in their data
- How individuals can access their personal data, as well as learn who will receive their data
- Opt-in or opt-out provisions for individuals
- Dispute resolution procedures

G. Review Your Consent Form

Consider using a consent form on your Web site. Make sure your consent form reflects all the possible uses for the data, including the possible transfer of the data via email.

My Clippings Folder

Close

You currently have no resources in your clippings folder.

Show Clippings