

Privacy Newsletter

SEPTEMBER 2001

www.mintz.com

PRIVACY NEWS

International Privacy Briefs

Japan • Japan's Cabinet has passed a privacy protection bill designed to set a legal framework for regulating the acquisition and dissemination of personal information for commercial use. The Japanese Government hopes to put the law in place during the current Diet session and begin enforcement of the law in spring of 2003. The proposed legislation is expected to affect the ways U.S. companies collect and handle personal information of Japanese nationals, and is also expected to affect the ability of Japanese companies to transfer personal information to companies outside Japan.

The proposed legislation stipulates five basic principles: the purpose for which personal data will be used should be specified and the use should not go beyond the specified purpose; collection of data should be made legally and properly; the data should be kept accurate and updated; security safeguards should be provided; and proper access to personal information should be given to the information subject. The law also bans the transfer of personal information to a third party without consent of the information subject.

Both public and private entities would be subject to the new laws, and entities that collect personal information about a particular person would, at the request of that individual, be obliged to release the information, correct mistaken data, or stop further dissemination of information concerning that person.

Providers of personal information will also be required to set up a system to handle public complaints and make swift responses. There are penalties attached for failure to comply with the provisions of the new law - a prison sentence of up to six months, or a fine of up to 300,000 yen.

(continued on page 2)

When a Website is a Financial Institution

by Adrienne C. Lavallee, Esq.

Although financial websites probably do not consider themselves financial institutions, they may be subject to regulation under legislation passed by Congress and signed by former President Clinton in 1999. Known as the Gramm-Leach-Bliley Act after the congressional authors, this law overhauled the U.S. financial services industry and opened up competition in banking, insurance and securities among the many different financial institutions throughout the country. It is very complex; but, virtually everyone agrees it is a necessary law that updates finance in a modern world.

Nine—that's right, nine—different federal regulatory agencies have responsibility for enforcing the law, including the Federal Trade Commission, the Securities and Exchange Commission, the Department of the Treasury and the Federal Deposit Insurance Corporation. All nine have issued regulations to implement the law.

Very importantly, Title V of the law addresses some of the potential risks to the privacy of personal information that can accompany increased information flow in the more integrated financial market provided for by the law.

Who is Affected by the Law?

The financial privacy regulations of the law apply to any "financial institution" that is significantly engaged in "financial services." As a website's financial services become more specific or individualized, the likelihood increases that it qualifies as a "financial institution." These definitions are hardly straightforward, however.

Rep. Billy Tauzin (R-Louisiana), Chairman of the House Commerce Committee, recently warned the SEC not to regulate Internet portals like Yahoo Finance and Motley Fool that merely provide financial information. The key issue for Chairman Tauzin is whether a financial website operates similarly to its traditional counterparts in the print, television and radio news media (*i.e.*, *Wall Street Journal*, *CNBC*, *WTOP-AM*). If so, Chairman Tauzin believes the website should not be subject to the implementing regulations just as traditional news media are not.

Although the SEC has indicated that it is not seeking to expand its jurisdiction, it is reviewing the results of a recently-conducted investors' survey to determine how financial websites influence their decisions. An SEC spokesperson recently stated that current Internet financial portal practices could give them a "salesman's stake" in the financial service industry. By that reasoning, a portal could qualify as a broker and come under the SEC's jurisdiction.

MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC

Privacy News

(continued from page 1)

Netherlands • On September 15, the Netherlands' Act on Protection of Personal Data (the "Act") comes into effect, implementing the EU Data Protection Directive. The Act imposes strict requirements on data controllers, defined as "natural or legal persons who determine the purposes of the processing and the means by which [the processing] is carried out." For commercial enterprises, the processing of personal data will generally meet the requirements of the Act if:

- ◆ The data subject has unambiguously consented;
- ◆ The processing is necessary for the taking of pre-contractual measures or the performance of an agreement to which the data subject is a party;
- ◆ The processing is necessary to further a legitimate interest of the data controller, unless the data subject's interests outweigh that of the data controller;
- ◆ The data is processed in a way that is compatible with the purpose for which it was collected;
- ◆ The data is adequate, relevant and not excessive; and
- ◆ The data controller implements adequate technical and organizational security measures to prevent the data from being lost or unlawfully processed.

For data controllers, the Act contains an important notice provision: the Act imposes an obligation on the data controller to notify the Netherlands Personal Data Protection Board in advance of any intended data transfers. This notification requirement enables data subjects to find out how businesses use data in their possession. Data controllers will not be required to report each processing operation individually, but may report a number of processing transactions at one time.

As with the EU Data Protection Directive, personal data may not be transferred from the Netherlands to a country outside the European Union if that country does not guarantee an adequate level of protection. The only exceptions to this rule are if the data subject unambiguously consents to the transfer, or if the transfer is necessary for the performance of a contract to which the individual is a party.

Australia • Australia amended its Privacy Act 1988 last December to make its provisions, previously applicable only to the public sector, applicable to the private sector as well. Under the changes to the Privacy Act, a set of National Privacy Principles (NPPs) are established which describe minimum standards for the handling of personal information.

(continued on page 3)

When a Website is a Financial Institution

(continued from page 1)

What Information is Affected by the Law?

The law's regulations governing financial privacy apply to private information about individuals who obtain financial products or services primarily for personal, family or household purposes. For example, a person's name, email address, and physical address all qualify as private information. Information that a financial institution collects about companies or individuals who obtain financial products or services for business, commercial or agricultural purposes is, therefore, outside the reach of the law's regulations. When a tax preparation firm counsels a corporation, this activity falls outside of the scope of this law.

In general, the law's regulations only govern the sharing of private personal information by a financial institution with a nonaffiliated third party. For example, this law applies to information flows between a bank and a credit reporting agency that the bank does not own or control. With the exception of certain notice obligations, the law's regulations place no restrictions on information-sharing between a financial institution and its affiliates if the information-sharing involves private personal information.

How Do You Comply?

Generally speaking, the law's regulations require the following of a financial institution:

- Provide initial and annual notice of privacy policies that include, among other items, the categories of private personal information collected, the categories of private personal information that might be disclosed, the categories of affiliates and nonaffiliated third parties to whom a financial institution discloses private personal information and the financial institution's policies with respect to sharing information about former customers;
- Produce an "opt-out" notice which means the individual is provided the opportunity to prevent the disclosure of private personal information to nonaffiliated third parties—such as the credit reporting agency referenced above—before any disclosures occur;
- Provide a reasonable opportunity to opt-out prior to disclosing private personal information to nonaffiliated third parties; and,
- Limit information-sharing practices with nonaffiliated third parties to comply with the law.

As the Internet burst onto the personal and institutional financial scene in the mid-1990s, it gave individuals access to unprecedented amounts of information. It also continues to give companies, including Web site operators, the ability to harness information in new ways to gain a competitive advantage. Just as traditional financial institutions have worked to comply with the new law, financial website operators should also consider the actions necessary for full compliance.

Privacy News

(continued from page 2)

The NPPs relate to how personal information is collected and used, and to whom it is disclosed. As with other national privacy acts, the NPPs require users of personal information to be open about their information practices and to maintain the accuracy and security of personal information. In addition, the NPPs place restrictions on offshore transfer of personal information similar to the EU Data Privacy Directive. The amendments to the Act are to go into effect on December 22, 2001.

The final guidelines promulgated under the Privacy Act are due to be published in mid-September, but have recently come under fire from big business, particularly the Australian Retailers Association. The ARA is concerned that there will not be enough time to adapt to the new guidelines prior to the busy holiday retail season. Other meetings with Australian business groups, particularly the Australian Banking Association, the ARA and the Australian Direct Marketing Association, have already resulted in a major redraft of the proposed guidelines—slashed from around 150 pages to 40 pages. Business groups would like to see the Government consider pushing back the operative effective date of the Act from the scheduled December date until sometime in 2002. Government officials have stated that there are no plans to delay applying the new law.

Domestic Privacy Briefs

The Future of Financial Privacy Legislation

Senator Phil Gramm (R-TX), always vocal in his opposition to new financial privacy legislation, announced Tuesday that he will retire at the end of his third term, which expires at the close of 2002. The Senator's departure could mean a smoother ride for tougher financial privacy legislation in the Senate. Legislation that would strengthen the privacy provisions of the Gramm-Leach-Bliley Act has been introduced in the House.

Assistant Secretary of Commerce Nancy J. Victory, who heads the Commerce Department's National Telecommunications and Information Administration, has indicated that the Bush administration has been working with the Federal Trade Commission on privacy issues. The Chairman of the FTC, Timothy J. Muris, has been meeting with privacy activists and industry representatives and is expected to announce his position on the issue within the next several weeks.

Privacy Laws Affect Clinical Trials

by Linda D. Bentley, Esq.

At a time of growing concern about the loss of personal privacy and the ease with which personal information can be disseminated to an unanticipated and sometimes unauthorized audience, many countries are taking steps to regulate the disclosure of this type of information. One of the areas of biggest concern relates to the protection of individually identifiable health information. Newly adopted laws and existing laws that have not been previously enforced may decrease the incidence of unauthorized use and disclosure of personal information, but they may also place unwanted obstacles in the way of biomedical research.

In the past, a proper written informed consent from a research subject was deemed all that was necessary to permit a researcher to use that subject's health data, but researchers now need to be mindful of the growing number of privacy laws that will require them to obtain other types of consents. Since a large number of clinical studies are performed in the U.S. and in Europe, some of the ways in which two laws governing the use and disclosure of personal health information in the U.S. and in the EU countries could affect clinical trials are identified below.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

In December 2000, the Department of Health and Human Services issued a final rule regarding standards for privacy of individually identifiable health information. Although the effective date was delayed to give the Bush administration a chance to review HIPAA's provisions and a guidance document issued on July 6, 2001 acknowledges that certain changes to the rule will be necessary, most covered entities must comply with the new requirements by April 2003. The rule applies to health care providers, which will include hospitals and physicians who participate in clinical trials, and to any research that involves the disclosure of protected health information (PHI).

Except in a limited number of circumstances, no health care provider may use or disclose PHI without first obtaining a patient's consent or authorization. The use of a consent is limited to situations involving treatment, payment or certain health care operations (TPO). Authorizations are required to use specified PHI for non-TPO purposes and to disclose PHI to third parties such as the sponsor of a clinical trial. While it is possible to de-identify data by removing eighteen specific identifiers and thus avoid having to get a HIPAA-compliant authorization, many studies will require follow-up that may make total de-identification unrealistic.

At present, research subjects participating in clinical research provide a written informed consent that meets the requirements of the Food and Drug Administration (FDA) or the Department of Health and Human Services (HHS), depending on the nature of the research. An informed consent that meets FDA or HHS requirements, however, is not the same as a HIPAA authorization. Unlike an informed consent, which HIPAA characterizes as a consent to participate in the research study as a whole, a HIPAA authorization is a consent for the research use or disclosure of PHI. HIPAA authorizations are customized documents that must include information about how the PHI will be used and to whom disclosures may be made. An authorization must also have an expiration date.

Under HIPAA, a patient's medical records are normally accessible to him or her unless a permitted exception applies. One of the exceptions applies to PHI created or obtained for a clinical trial. In that situation, the individual's access right is temporarily suspended while the clinical trial is in progress, provided the research participant agrees to this denial of access when consenting to participate in the clinical trial. The access right is reinstated, however, once the trial is completed.

(continued on back)

Privacy Laws Affect Clinical Trials

(continued from page 3)

EU Privacy Directive

In October 1995, the European Union (EU) adopted Directive 95/46/EC, which relates to the processing of personal data and the free movement of such data. The Directive permits free movement of the data within and between the fifteen EU member states, and limits transfer of the data to non-EU countries unless they provide adequate levels of protection for such information. The Directive requires member states to enact their own laws or regulations to implement the Directive, but not all have yet done so.

Clinical research, although not defined, falls within the purview of the Directive. The sponsor of the study would probably be considered a controller, which is an entity "which alone or jointly with others determines the purposes and means of the processing of personal data." Personal data is defined broadly as any information relating to an identified or identifiable natural person, and processing of data includes activities such as the collection, recording, organization, storage, use, and disclosure by transmission of personal data. Unless an individual has provided unambiguous consent to the processing of the data or another specific situation exists, no processing may occur. The processing of health information receives special treatment and may not occur without a data subject's explicit consent, unless a member state does not recognize such a consent. The Directive does not indicate what constitutes "unambiguous consent" although consent is defined as any "freely given specific and informed indication of [a data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed."

Transfer of the data to non-EU countries, which do not ensure an adequate level of protection, is prohibited, although the Directive would permit such a transfer under several circumstances, including the data subject giving his consent unambiguously to the proposed transfer. At the current time, only Switzerland and Hungary satisfy the adequacy standard. U.S. companies have the option, however, of voluntarily certifying compliance with a so-called safe harbor developed by the U.S. Department of Commerce and the EU. To date, very few U.S. companies have followed the safe harbor route, probably because of the costs associated with meeting the requirements and an unwillingness to open themselves up to the safe harbor enforcement provisions. As a result, it is likely that most companies performing clinical trials in the EU countries will try to rely on unambiguous consents.

www.mintz.com

One Financial Center
Boston, Massachusetts 02111
617 542 6000
617 542 2241 fax

11911 Freedom Drive
Reston, Virginia 20190
703 464 4800
703 464 4895 fax

701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
202 434 7300
202 434 7400 fax

666 Third Avenue
New York, New York 10017
212 935 3000
212 983 3115 fax

Mintz Levin and ML Strategies provide legal, legislative and consulting expertise on privacy as it relates to many issues. If you would like further information, please contact the Mintz Levin attorney who regularly handles your legal affairs, or one of the attorneys or senior professionals listed below.

Privacy Regulation

Neil H. Aronson617 348 1809
Franklin Blackstone III703 464 8144
Amy L. Bushyeager202 434 7479
Gordon R. Caplan.....212 692 6702
John M. Delehanty212 692 6703
Robert Duggan617 348 1780
Christopher J. Harvie202 434 7377
Paul A. Hughes203 787 6320
Julie E. Korostoff.....617 348 1638
Fernando R. Laguarda.....202 434 7347
Cynthia J. Larose.....617 348 1732
Adrienne C. Lavallee202 434 7362
Frank J. Marco203 787 6310
Bruce D. Sokler202 434 7303
Howard J. Symons.....202 434 7305
Ivan S. Wool212 692 6757
Wayne M. Zell.....703 464 8135

Health Privacy

Michael D. Bell202 434 7481
Linda D. Bentley617 348 1784
Susan W. Berson.....202 661 8715/212 692 6750
Raymond D. Cotton202 434 7322
Erin Lewis Darling202 434 7478
Hope S. Foster202 661 8758
Elizabeth Brody Gluck617 348 1871
Ellen L. Janos617 348 1662
Peter M. Kazon202 661 8739
Rebecca A. Matthews203 787 6329
Laura J. Oberbroeckling202 434 7333
Eric S. Tower202 434 7344

Privacy Litigation

Susan L. Burke202 661 8707
Michael S. Gardener617 348 1642
Kevin M. McGinty.....617 348 1688
Laurence A. Schoen.....617 348 1764

Employment Privacy

Jennifer B. Rubin 203 787 6324
Teresa Burke Wright202 434 7341

Legislative Privacy Strategies

Patrick A. Hope.....202 434 7407
David J. Leiter.....202 434 7346

Public Relations Strategies

Jason D. Glashow617 348 1667

157 Church Street
New Haven, Connecticut 06510
203 777 8200
203 777 7111 fax

MINTZ LEVIN
COHN FERRIS
GLOVSKY AND
POPEO PC

ML
STRATEGIES