Global Privacy Law Update

As data processing technology develops rapidly, so too does the law to protect individuals' private information. Internationally, countries have passed increasingly stringent privacy protection laws to foster trust among the public, as well as to maintain compliance with other countries’ legal regimes. While the goal of most of these laws is to protect personal information and obtain consent for its use and disclosure, requirements can vary significantly among the different nations, as well as within each country’s subdivisions. With enforcement of privacy law on the rise as well, it becomes important for transnational businesses to understand and make reasonable efforts to comply with each country's laws. This Update provides a brief primer on a number of the recent privacy law developments around the globe.

Canada

On January 1, 2004, the final stage of Canada’s sweeping privacy law went into effect. The 2001 Personal Information Protection and Electronic Documents Act (PIPEDA) protects all personal information collected, used, or disclosed by an organization or business while engaged in a commercial activity. The law defines “personal information” as any data that identifies an individual, but not a person’s name, title, or business phone number and address. “Commercial activity” includes making and providing a product or service that is commercial in nature, including the private delivery of health care services.

Complying with PIPEDA requires that a company subject to the Act inform individuals of their privacy rights. It also requires that a business provide data subjects with the opportunity to know what personal information the company will collect, why the information is collected, the purpose for which it is collected, and how it will be used, disclosed, and protected. Businesses must obtain consent each time they use personal information a new way or disclose it to a third party.

Consent is key to PIPEDA, although organizations may also infer consent in a limited number of circumstances. For example, a lab may infer consent when it sends test results to a provider, because that is what a reasonable patient would expect. Express oral or written consent would still be required, however, if any disclosure was not directly related to the provision of care.

In the research context, PIPEDA does not always require consent. If the researcher or organization (1) uses or discloses the information for purely statistical or scholarly
purposes, or for purposes that cannot be achieved without its use or disclosure; (2) uses the information in a manner that will ensure confidentiality; (3) cannot practically obtain the subject’s consent; and (4) informs the Office of the Privacy Commissioner of Canada before using or disclosing the information, then PIPEDA does not require express consent. PIPEDA still does permit manufacturers of pharmaceuticals to report adverse drug reactions as legally required under the Food and Drugs Act.

PIPEDA also requires that businesses store personal information securely and limit access to it. Businesses must inform individuals of their procedures for handling personal information. This can be accomplished by posting notices, distributing brochures, and providing an opportunity for an individual to discuss these practices. Organizations must also protect temporary records as they would protect permanent ones.

The privacy policies that companies develop in response to PIPEDA will necessarily vary depending on the company’s size and type. All of entities subject to the Act, however, should appoint a privacy officer. The standard policy should also include measures to protect the physical security of the information (locking cabinets, limiting access), technological systems (encryption, firewalls, passwords), organizational efforts (security clearance, confidentiality agreements), and staff training regarding privacy procedures and maintenance.

The Act also provides individuals with certain rights. Businesses must allow data subjects to access records containing their personal information, tell individuals how they can access the information, inform individuals how they can make changes to the information, and notify individuals about how they can complain about a business’s privacy practices. While PIPEDA does not explicitly define “access,” the Canadian government has expressed its intent that individuals be able to view their records in a way that they understand.

Under a limited number of circumstances, PIPEDA does permit businesses to deny an individual access to a record. PIPEDA exempts a business from allowing access if (1) that would reveal personal information about a third party who does not consent to the disclosure and the third party’s information cannot be redacted; (2) the business has a reasonable expectation that the information could harm or threaten the life of another person and it cannot sever the third party information; (3) a privilege protects the information; or (4) the information would reveal confidential commercial information. A business cannot, however, deny access because it believes that the information might harm the individual requesting access.

Companies must also be aware of the interplay between the provincial law and PIPEDA. The federal law does not apply within a province if that province has a substantially similar law. To date, the Canadian government has only recognized Quebec as having a substantially similar law, although Alberta’s and British Columbia’s laws contain the same principles and those provinces hope to have the federal government recognize their laws as similar in the near future. Even if the province’s law is substantially similar, PIPEDA still applies to all personal information sent outside of the province by organizations and business subject to the Act.

Many companies are currently struggling to implement the new federal requirements. The Privacy Commissioner estimates that only 20 percent of organizations are compliant with the law. While the new Commissioner (appointed in December 2003) has stressed that she will be more flexible and cooperative in working with the private sector on compliance issues, businesses need to take steps to show that they are making a reasonable effort to conform to the law’s requirements.

European Union (EU)
Finding of Adequacy The European Commission (EC) declared the Baliwick of Guernsey safe for personal data export from EU countries in February 2004. Guernsey now joins the ranks of a
limited number of countries approved by the EC as providing an adequate level of protection of personal information. The decision allows for the transfer of information from EU and European Economic Area (EEA) member countries to a third country without requiring any further safeguard. The other countries that the EC has designated as providing adequate protections are Argentina, Canada (partial approval), Hungary, and Switzerland. It is likely that the EC will soon also grant approval to the Isle of Man.

**United Kingdom** In one of its first interpretations of the Data Protection Act (the Act), Durant v. Financial Services Authority [2003] EWCA Civ 1746, the UK Court of Appeal denied an individual access to his records at a financial institution. After unsuccessfully suing Barclays Bank, Mr. Durant sought access to various records he believed would assist him in reopening claims against the bank. Mr. Durant asked the Financial Services Authority (FSA) to assist him, and although the FSA provided him with some records, it did not permit access to all of the manual files and it redacted some of the information in the computerized documents.

The court first considered what constitutes “personal data” and noted that even if the record includes a person’s name, it is not necessarily personal. To be personal, the information must be biographical and go beyond mere involvement in a matter, and the focus of the information should be on the individual seeking access. Personal data is information that affects a person’s privacy in his personal or professional life. Consequently, the files in question did not contain personal information because they related to Mr. Durant’s complaint and the FSA’s subsequent investigation, not to Mr. Durant personally.

Next, the court interpreted the meaning of a “relevant filing system.” The court concluded that this is a filing system that clearly indicates whether the files contain specific personal information and where the files are readily accessible. Here, the bank did not structure the manual files so as to fall within this definition.

This decision will impact future requests for information under the Act. While it may not reduce the number of requests for information that a company receives, it will require businesses to thoroughly consider whether the requested information is clearly personal information within a relevant filing system. Although the court may have reduced the scope of personal information, the concept remains very broad.

**India**

Indian cities such as Mumbai, Delhi, and Bangalore are increasingly becoming frequent destinations of international companies’ data because of the low cost of labor relative to the technical expertise of the workforce. For example, an estimated 80 percent of the jobs outsourced in the US go to India. Yet as the outsourcing of business operations to India becomes increasingly widespread, concerns about whether the personal information processed there remains private increase as well. Reports of fraud are common, and last year’s incident where a call center employee went on a shopping spree after stealing the credit card number of a caller from the US sparked considerable media attention.

The US and EU member countries with business processing outsourcing (BPO) work and call centers in India have pressured the government to pass legislation to protect personal information. Opponents of outsourcing in the US and Europe have frequently used India’s lack of protection of personal information as a main reason to curb BPO operations, and in the US some Members of Congress have introduced legislation designed to protect private information sent to other countries. Some business groups, however, argue that these efforts are really intended to provoke greater protectionism.

The Indian government has responded to this controversy by announcing that it would develop legislation to protect personal data and to foster trust among businesses and consumers. The Indian government is working with the National Association for Software Service Companies (NASSCOM), the
country’s primary trade association for the information technology sector, in drafting the privacy protection bill. The proposed legislation applies to financial transactions, unsolicited mass emails, and unauthorized access to personal data. The government may amend the Information Technology Act of 2000, which only deals with unauthorized access to computer systems and data theft, rather than create an entirely new legislative framework. It is expected that the new proposal will pass soon and the government will implement the law by the fall. After the new law is in place, the government plans to enter into negotiations with the EU to designate India as a country that offers an adequate level of protection of individual’s personal information.

**Japan**

In May 2003, Japan enacted a number of new privacy laws directed at the protection of private information. The legislation was passed after considerable controversy about possible interference with the media. Opposition to the new laws continues, with media groups charging that the reforms allow the government to control reporting under the guise of protecting privacy.

These comprehensive measures seek to prevent companies from illegally obtaining personal information or disseminating information to third parties. The penalties for breaking the new laws can be harsh, with some violators facing prison terms of up to six months or fines of up to 300,000 yen if they leak personal information. The laws also give individuals the right to request that direct marketers share the information that they possess, that companies correct that information, and that they stop using the information altogether.

One of these reforms directs the Cabinet Office to create a database of consumer complaints of improper uses of personal information. The government intends for the database to deter corporate misuse of its customer information. The Cabinet Office will post the complaints on the Internet. Another of the laws requires that businesses only use personal data for predefined purposes, that they notify individual subjects that they will use the information, and that businesses gain consent before transferring personal information to a third party. The government included a provision exempting media groups and academic research organizations from this provision. The Japanese law, however, does not explicitly prohibit the transfer of information to other countries without similar privacy laws.

Japan is also working on a new provision directed at the telecommunications industry after a highly publicized leak. Last December, a broadband Internet service provider employee leaked approximately 4.5 million subscribers’ personal information. This internal security lapse captured the public’s attention and highlighted the security threats within the information technology sector.

A Japanese government panel has recommended a proposal that would require the private and public sectors appoint officers to be responsible for privacy protection. Officers would establish measures to prevent access to computer systems to prevent information leaks and to address them when they do occur. Officers would also take a public pledge to address customer complaints about the treatment of their personal data. The draft legislation further requires that companies do not use private information for anything other than core business activities. These draft recommendations are expected to become part of the final law in early 2005.

---

We hope that you find this brief summary helpful. This is only a general summary and should not be construed as providing legal advice. If you would like more information, please feel free to contact:

**John Bentivoglio**
202.942.5508
John_Bentivoglio@aporter.com

**Nancy Perkins**
202.942.5065
Nancy_Perkins@aporter.com