AN INTRODUCTION TO THE EU DIRECTIVE ON THE PROTECTION OF PERSONAL DATA

By Peter K. Yu

Introduction

The Internet and new communications technologies have made shopping more convenient than ever. Online shopping is fast, easy and reliable. It even may offer special discounts that are not available elsewhere.

However, e-shoppers are sometimes concerned about the misuse and mishandling of their personal data. Who wants strangers to know his home address and social security number? Who wants others to analyze her reading habits and medical history? Who wants to receive unsolicited junk e-mails that fill up his mailbox storage space?

In 1995, the European Union enacted the EU Directive on the Protection of Personal Data ("EU Directive"), which requires all member states to implement legislation to protect the right to privacy with respect to the collection, processing, storage and transmission of personal data.

Defining personal data broadly as any information relating to an individual, the Directive aims to develop a high level of data privacy within the European Union. It also seeks to promote the free flow of personal data by harmonizing privacy laws among the 15 member states (Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Portugal, Spain, Sweden and the United Kingdom). Focusing primarily on the private sector, the EU Directive allows for various limited exceptions, including public security, defense, state security, law enforcement and personal or household activities.

The EU Directive further prohibits the transfer of personal data to non-EU countries that do not meet the European "adequacy" standard for data protection. To protect American businesses against the possible interruptions in data transfer concerning their business dealings with European companies and the potential prosecutions by European authorities under European privacy laws, the United States negotiated with the European Commission for a "safe harbor" framework, which allows U.S. companies to satisfy the European "adequacy" standard while maintaining their traditional self-regulatory approach to data protection.

In July 2000, the European Commission approved of the safe harbor framework and issued a decision that the framework meets the European "adequacy" standard. To allow companies to decide whether they would participate in the safe harbor and to implement information practices that will be needed to comply with the framework, the European Union granted U.S. companies a one-year moratorium, which ended on July 1, 2001.

An Overview of the EU Directive

Under the EU Directive, every business is required to ensure that the personal information collected from its customers is:

- processed fairly and lawfully;
- collected and processed for specified, explicit and legitimate purposes;

- adequate, relevant and inexcessive in relation to the purposes for which the data are collected or processed;
- accurate and updated as necessary; and
- kept in a form that permits identification of individuals for no longer than is necessary.

In addition, the business must tell its customers who the controller (or the person in charge of the data) is, whether the customers are obligated to provide their personal information, the right of access to such information and the right to correct any inaccuracies in the data.

Once collected, these data may not be processed unless the customer has unambiguously given his or her consent or unless processing is necessary:

- for the performance of a contract involving the customer or the implementation of precontractual measures at the customer's request;
- for compliance with the controller's legal obligation;
- to protect the customer's vital interests;
- for the public interest or the exercise of official authority vested in the controller or a third party to whom the data are disclosed; or
- for legitimate interests pursued by the controller or a third party, except where the customer has greater privacy interests.

In the event personal data are mishandled, the EU Directive grants an individual a right of redress. Remedies will be determined by national law and may vary from one member state to another.

In addition, the EU Directive requires all member states to establish an independent supervisory authority to oversee the regulation of personal data. This supervisory body possesses independent power to investigate and ban data processing activities, to order the destruction of personal data, to block data transfer to third parties, to hear complaints from data subjects, and to issue regular public reports. Unless statutory exemptions apply, the controller must notify this supervisory body before carrying out any automated processing operation.

Impact on U.S. Companies

To prevent circumvention of the EU Directive and creation of "data havens" outside the European Union, the Directive prohibits the transfer of personal data to non-EU countries that do not meet the European "adequacy" standard for privacy protection.

Whether a country will meet this adequacy standard depends on all the circumstances surrounding the data transfer operation. Particular consideration will be given to the nature of the data, the purposes and duration of the processing operation, the country of origin and country of final destination, the rules of law in force in the country in question and the procedural rules and security measures that are compiled in that country.

This provision is particularly alarming to U.S. businesses, for it can cut off all personal data flows from the European Union. Such disruption would affect a large variety of trans-Atlantic business activities, including personal banking and brokerage transactions, airline and hotel reservations, Internet sales, credit checks, credit card purchases and inter-office communication between EU and non-EU branches of a multinational corporation.

Notwithstanding this harsh provision, the EU Directive offers some exceptions:

- the data subject has unambiguously given his or her consent to the data transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract in the interest of the data subject between the controller and a third party;
- the transfer is necessary or legally required in the public interest or for legal claims;
- the transfer is necessary to protect the vital interests of the data subject;
- the transfer is made from a register that is intended to provide information to the public and that is open to the public or any person having a legitimate interest; or
- the controller is able to demonstrate the existence and applicability of safeguards sufficient to protect the privacy of the data subject.

Differences Between the U.S. and the EU Approaches to Data Protection

Unlike the European Union, the United States traditionally has adopted a different approach to data protection.

First, the European Union embraces privacy as a fundamental human right and thus considers comprehensive legislation as the most appropriate means to protect personal information. Such an approach requires the creation of government data protection agencies, registration of databases with those agencies and approval before the processing of personal data. By contrast, many Americans believe in the free market and are constantly suspicious of government intrusions. Thus, prevailing U.S. opinion prefers a sectoral approach that relies on a mix of legislation, administrative regulation and industry self-regulation (through code of conducts developed by industries as an alternative to government regulation).

Second, the First Amendment to the U.S. Constitution imposes limits on the government's ability to regulate the flow of information, including personal data. Comprehensive legislation like the EU Directive would undermine significant interests protected by the First Amendment. Thus, U.S. privacy laws tend to be carefully drafted so that they are narrowly tailored to the type of information (such as video rental records and driver's license records), victims (such as children) and business (such as credit reporting agencies, financial institutions and health-care organizations) the laws are designed to regulate.

Third, the United States does not have a specific government data protection agency. Instead, data privacy is supervised by a large and diverse array of government agencies, including the Department of Commerce, the Department of Health and Human Services, the Department of Transportation, the Federal Reserve Board, the Federal Trade Commission, the Internal Revenue Service, the National Telecommunications and Information Administration, the Office of the Comptroller of the Currency, the Office of Consumer Affairs, the Office of Management and Budget and the Social Security Administration.

U.S. Safe Harbor Framework

To reconcile these differences, the U.S. Department of Commerce reached an agreement with the European Commission on a "safe harbor" framework. This framework provides predictability and continuity for U.S. companies transmitting personal information from Europe. It also eliminates the need for prior approval of data transfers and benefits small and medium enterprises by offering a simpler and cheaper means of complying with the EU Directive.

Consistent with the U.S. self-regulatory approach, the safe harbor framework allows companies to decide whether they want to participate in the framework. To qualify for the safe harbor, a business must notify

the Department of Commerce in writing annually and declare publicly in its published privacy statements that it adheres to the Safe Harbor Principles, which are summarized below.

The Department of Commerce will maintain and make publicly available a list of all organizations that have self-certified. If a business that has self-certified persistently fails to comply with the Safe Harbor Principles, the Department of Commerce will indicate in the list the business's noncompliance and thus ineligibility for the safe harbor benefits. Such noncompliance may lead to sanctions under section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive trade practices.

There are two ways to adhere to the Safe Harbor Principles. First, a business can develop its own self-regulatory privacy program that conforms to the Principles. Alternatively, it can participate in a self-regulatory privacy program that adheres to the Principles.

The seven Safe Harbor Principles are summarized as follows:

1. **Notice.** The business must clearly tell its customers why it collects their personal information, how it plans to use such information, whom they can contact with inquiries and complaints, the types of third parties to which the business intends to disclose their personal information, and the choices and means through which they can restrict the use and disclosure of such information.

2. **Choice.** If the business wants to disclose to a third party the personal information of its customers or to use such information in a way that has not been previously authorized, the business must give the customers an opportunity to opt out of such disclosure or use. For sensitive information—such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and information concerning health or sex life—the business also must provide an affirmative or explicit opt in procedure.

3. **Onward Transfer.** To disclose personal information to a third party, the business must comply with the notice and choice principles. In addition, the business must limit its disclosure to third parties that subscribe to the Safe Harbor Principles or that are subject to the EU Directive or an "adequacy" finding. Contracts ensuring that the third party will offer the same level of protection as required under the Safe Harbor Principles will satisfy this principle.

4. **Security.** The business must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

5. **Data Integrity.** All personal information must be relevant for the purposes for which it is to be used. The business must not process any personal information in a way that has not been previously authorized and should take reasonable precautions to ensure that data are reliable for their intended use, accurate, complete and current.

6. **Access.** Each customer should have reasonable access to the stored information about him or her and an opportunity to correct, amend or delete any inaccuracies, except where the burden or expense of providing access would be disproportionate to the risks to the customer's privacy or where the rights of other persons would be violated.

7. **Enforcement.** The business must provide an independent, readily available and affordable dispute resolution mechanism for investigating and resolving customers' complaints and disputes. It also must institute a procedure for independently verifying its compliance with the Safe Harbor Principles. In addition, the business must be committed to remedy problems arising out of its failure to comply with the Principles. To ensure compliance, the dispute resolution body must be

> able to impose sanctions that are sufficiently rigorous. Examples of such sanctions include publicity for findings of non-compliance, deletion of data, suspension from membership in the privacy program, injunctive orders and damages. A privacy seal program that incorporates and satisfies the Safe Harbor Principles will satisfy this principle.

As in the EU Directive, the Safe Harbor Principles allow for several exceptions. These exceptions include national security; public interest; law enforcement; conflicting obligations created by, or explicit authorizations stipulated in, statutes, regulations or case law; and exceptions and derogations provided by the EU Directive or adopted by the member state from which the personal data originate.

Conclusion

Since the passage of the EU Directive, commentators have noted how the European Union has shaped the global privacy protection debate and how the EU Directive would impose on the United States a protective scheme that is inconsistent with the American tradition. However, as indicated by the European Commission's approval of the safe harbor framework, the European Union is hesitant to insist on its legislative approach if such insistence would jeopardize its economy and e-commerce development. After all, the United States provides a very lucrative market for the European Internet industries. Sanctions on U.S. companies would hurt the European Union as much as it would hurt the United States.

When evaluating the EU legislative approach, one must not forget that the EU Directive was drafted more than 10 years ago. To some extent, the Directive was outdated even before it entered into force. Using terms such as "controller" and "data subject," the EU Directive assumes a top-down architecture that is more applicable to big corporations and mainframe computers than to individuals, small and medium enterprises and a network of personal computers and laptops. Thus, it would be interesting to see how the EU Directive will evolve in light of the challenges posed by the Internet, the e-commerce explosion and the proliferation of automated data-transfer devices such as cookies and web "bots."

In stark contrast to the rigid EU legislative approach, the U.S. self-regulatory approach is more adaptable to new communications technologies. Such an approach also may promote the development of technical standards and default settings, which supplement nicely the existing privacy legislation and self-regulatory mechanism. The United States may have started in a defensive position. Yet, it may very well have the final say over how the global community should protect data privacy.

Peter K. Yu is a member of the GigaLaw.com Editorial Board and the executive director of the Intellectual Property Law Program and deputy director of the Howard M. Squadron Program in Law, Media & Society at Benjamin N. Cardozo School of Law in New York City. He is a research associate of the Programme in Comparative Media Law & Policy at the University of Oxford and has written on a variety of legal topics. He is licensed to practice law in the state of New York. E-mail: peter_yu@.msn.com.