

DEALING WITH DATA PRIVACY PROTECTION: AN ISSUE FOR THE 21ST CENTURY

Fritz H. Grupe, Ph.D., William Kuechler, Ph.D., and Scott Sweeney, Ph.D.

In many surveys, Americans identify invasion of privacy as a primary concern. Nonetheless, newer electronic technologies, such as biometric monitoring, Web site tracking, vehicle tracking, basket-level purchase tracking, charge card usage recording, personal information data-base sales, release of government data to private corporations, facial identification, DNA testing and record keeping, smart card usage, telephone records, e-mail monitoring, and the like, intrude themselves into our private lives on an ever-expanding basis. It seems that every company and every governmental agency has an interest in knowing what we do, what we like and dislike, what we read, how long we sustain interest in something, which stores we frequent, and what we ignore. The European Union (EU) and other countries outside the EU are taking an approach to privacy that companies with an international presence must address to maintain compliance with that approach.

FRITZ H. GRUPE, Ph.D., is a professor of information systems at the University of Nevada, Reno.

WILLIAM KUECHLER, Ph.D., is an assistant professor of information systems at the University of Nevada, Reno.

SCOTT SWEENEY, Ph.D., is an associate with the brokerage services firm CB Richard Ellis.

On January 11, 2001, the attorney generals of 44 states and the Federal Trade Commission (FTC) submitted their legal opinions to the Bankruptcy Court of Boston that the online children's toy store, Toysmart, a subsidiary of the Disney Corporation, should be prevented from selling their customer list while it was in bankruptcy status. Prior to entering bankruptcy, Toysmart had indicated in their privacy policy that no data would be released to other companies. The primary legal basis for their opinion was that the Children's Online Privacy Act of 1998 requires parental consent for the release of data pertaining to the concerned children. The day after the FTC lawsuit, Disney stepped in and helped dispose of the controversy by paying \$50,000 to obtain the list and keep it confidential.

The reaction of the American and European audiences to this minor case illustrates the wide gulf in cultural-political perceptions concerning the protection of privacy data. To Americans the case was a great success on two points. First, existing congressional legislation ensured an "adequate" level of protection of the personal data involved. Second, the parent firm was self-regulated enough to prevent dispersion of the information by making a financial sacrifice. However, to appalled Europeans, especially the data protection commissioners of the EU member countries, the case is evidence in favor of their own point of view. If it takes 44 state attorney generals and the FTC to block the actions of one minor courtroom of America, how could this company possibly ensure "adequate" personal data protection on the Internet?¹

The DPD grants individuals broad rights previously not available, including the right to seek compensation for damages incurred by violations of these principles.

DATA PRIVACY IN THE EUROPEAN COMMUNITY

The European Commission (EC) Data Protection Directive and similar comprehensive legislation found in other nations are a culmination of work passed down over the ages. Some may even argue traceability to other conventions on human rights or even Articles 4 and 11 of John Stuart Mills' *The Declaration of the Rights of Man and of the Citizen*.

As early as 1968, the first European Working Party of EC ministers met to consider data protection rights and to determine whether existing human rights conventions and domestic laws were sufficient to protect data privacy. In 1981 the ministers signed Convention 108, "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." More than 24 countries signed Convention 108. Chapter 3, Article 12 of the Convention governs transborder data flows (TBDFs); and it allows nations to block data flows to another party if there is not equivalent privacy protection. Considering that Convention 108 was developed with the lowest common denominator in existing data protection laws (and in the case of Italy and Greece, no applicable laws whatsoever), one may have divined at the time that this was not the end of the matter.

The EC issued a particularly strict draft concerning data protection in September, 1990. Simitis describes the long process from draft to signature that lasted over five years.² As with many battles within the Council of Ministers, lines were drawn between the centralizing power of Brussels and the sovereign powers of the member states. Lost in the political rhetoric was whether it was even wise, despite the good intentions, to set up a huge new bureaucratic body within member states to review applications, collect fees, regulate and monitor compliance, and impose penalties, for example, in the rigid model of France's Commission Nationale de l'Informatique et des Libertés (CNIL). Eventually, this colorful legislative process led to Directive 95/46/EC, October 24, 1995, "Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data" and Directive 97/66/EC, December 15, 1997, "Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector." Signatories to the Data Protection Directive 95/46/EC were required to comply by October 24, 1998.

Transborder data flow (TBDF) refers to "a complex set of issues that have come to the forefront as a result of the electronic transfer or exchange of information across national boundaries. TBDFs involve the flow of digital information across borders for the storage or processing in foreign computers."³ TBDFs outside of the 15 EU member countries are regarded as a "transfer of information to third countries."

DATA PRIVACY PROTECTION PRINCIPLES

As of March 1, 2001, a major, new factor entered into the way in which international companies must treat data on their employees and customers. This factor is the Data Protection Directive of 1998 (DPD), which took force at that time. It became mandatory to enact the European Directive into national legislation in 1998. Each EU country is, of course, sovereign; and since it is the national law that applies, each country's laws must be harmonized with regard to principles outlined in the Directive. The DPD controls how, within the European Union, data regarding living individuals can be acquired, stored, transmitted, and processed; and these controls have considerable impact not only on computerized records but also on data stored in all formats, including paper. The DPD has a significant impact on all companies doing business in the eleven member countries of the EU, even if their home office is in the United States or any other country outside of the EU. With some variation, the United Kingdom has enacted similar requirements.

Information about data subjects is regulated according to eight *data protection principles* that guide the formulation of more specific procedures and standards that control how data will be collected, who can be involved in the processing of data, and how data can be used and distributed. The DPD grants individuals, who are sometimes referred to as *data subjects*, broad rights previously not available, including the right to seek compensation for damages incurred by violations of these principles. One set of principles in relation to the quality of data require that data be:

- Processed fairly and lawfully.
- Collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical, or scientific purposes shall not be considered as incompatible provided that

If the United States congress decides to adopt legislation compatible with the EU Data Protection Directive, it may want to start with the United Kingdom's regulatory model.

member states provide appropriate safeguards.

- Adequate, relevant, and not excessive in relation to the purposes for which they are collected or for which they are further processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data that are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- Kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member states shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical, or scientific use.

In addition, there are principles that guide how data regarding the data subjects may be processed.

Member States shall provide that personal data may be processed only if:

- The data subject has given his consent unambiguously; or
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject entering into a contract; or
- Processing is necessary for compliance with a legal obligation to which the controller is subject; or
- Processing is necessary in order to protect the vital interests of the data subject; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed,
- Except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).

Some 60 countries have either implemented the data privacy protection principles in law or are considering doing so.

Jacqueline Klosek provides a comprehensive summary of the DPD as enacted by the various EU member states.⁴ "Due to the fact that

European Union member states were given considerable freedom in transposing the Data Protection Directive into national law, there are some disparities among the national measures that have been adopted in the various member states. As such, entities dealing with personal data in Europe will need to be well acquainted not only with the European Directive but also with the implementing legislation of the 15 member states."

The United Kingdom's Data Protection Act is probably the most harmonious with America's position on data protection issues, seeking for the time being no more than compliance with the convention's minimum requirements. If the United States congress decides to adopt legislation compatible with the EU Data Protection Directive, it may want to start with the United Kingdom's regulatory model. The information commissioner (formerly data protection commissioner) maintains the public register of data controllers throughout the country, and the registration form can be accessed online or by telephone. The fee for notification is £35, renewed annually, with any changes made within 28 days. Organizations must register if they are processing personal information for the following purposes:⁸

- Private investigation
- Health administration
- Policing
- Crime prevention and prosecution of offenders
- Legal services
- Debt administration and factoring
- Trading or sharing in personal information
- Constituency casework
- Education
- Research
- Administration of justice
- Consultancy and advisory services
- Canvassing political support among the electorate
- Pastoral care
- Provision of financial services and advice
- Credit referencing
- Accounts and records

The following organizations are exempt from notification if they are processing for the following purposes:

- Personal, family, and domestic
- Public registers
- Not-for-profit organizations (small clubs, voluntary organizations, church administration, and some charities)

The British government is now considering revising the regulations since “the benefits to public health research of passing on data without consent (may) outweigh the rights of patients to have a say.”

- Core business purposes (small business)
- Staff administration
- Advertising, marketing, and public relations (for one's own firm only)
- Administration of customer and supplier records

However, data controllers must comply with the Data Protection Act even if they are exempt from formal notification. TBDFs are covered on the purpose form, and the data controller of the organization must indicate whether personal data is transferred outside of the European Economic Area (EEA). The names of the countries are listed unless over ten are indicated (worldwide). Posting information on a Web site constitutes worldwide transfer.

What has been the effect of the Office of the Information Commissioner (OIC) on business activities? From middle 2000 to middle 2001, the OIC investigated almost 900 complaints and secured 21 convictions.⁵ Most of the convictions were for workers abusing their data processing duties and tapping into a firm's database for their own ends. The OIC's biggest worries have little to do with the processing done by private firms; but governments plan to put a greater amount of their services online, *police records*, and European plans to make Internet service providers retain customer data for up to seven years for security purposes. The OIC also administers the Regulations of Investigatory Powers Act of October, 2000, which regulates how employers monitor employee e-mails and Internet access. While most United Kingdom firms seem to be unaffected by the data protection requirements thus far, there are some major differences with regard to data operations and electronic commerce compared to firms in the United States. For example, unlike in the United States, it would be illegal for United Kingdom corporations to sell customer data without first informing those on the list.⁶ A similar issue has surfaced in the field of medical research. For example, due to the Data Protection Act, many hospitals are no longer automatically passing on information to the United Kingdom's National Cancer Registry, one of the best in the world.⁷ Legally, the confidential information can only be supplied with the patient's consent. The British government is now considering revising the regulations since “the benefits to public health research of passing on data without consent (may) outweigh the rights of patients to have a say.”

The European position, now taken up by numerous other countries, can be characterized as being:

- Protective of personal rights with respect to data about individuals
- Restrictive regarding the flow of personal data out of the country of origin, except to other countries honoring the data privacy principles (DPP)
- A view of the people as citizens who are in control of their personal data
- Regulated by general laws, principles, procedures, and standards adopted to oversee the collection of data by governmental agencies established for this purpose

DATA PRIVACY IN THE UNITED STATES

The American position, on the other hand, can be characterized as being:

- Unprotective of data about individuals collected by businesses and government
- Unrestricted flow of data among companies
- A market-driven view of people as consumers under which data is seen as a saleable, usable commodity that belongs to the corporation
- Reliance on self-regulation by companies to respect an individual's privacy
- Regulated by specific pieces of legislation (i.e., by sector) that relate to particular aspects of privacy, but not to privacy generally

The United States has not had general privacy protection safeguards in place that are equivalent to those enacted in conjunction with the DPP. The United States has enacted specific legislation with regard to particular problem areas. Often, this has left open the question of privacy in other sectors and problem areas. Naturally, groups such as Computer Professionals for Social Responsibility, the Privacy Coalition, and the like have called for broader protections. [Exhibit 1](#) displays a few of the major pieces of legislation that bear on some aspect of privacy. By the time the EC's DPP took effect, online sales had tripled from about \$3 billion in 1997 to approximately \$9 billion in 1998.⁸ Prior to the directive, most information systems managers considered restrictions on transborder data flows as one of their most minor issues.⁹

In addition to the adjustment companies make to United States laws, self-regulatory efforts such as the TRUSTe and BBBOOnline Privacy Seal programs, intended to reduce consumer

EXHIBIT 1 United States Legislation
Offering Some Privacy Protection

Fair Credit Reporting Act (1970)
 Privacy Act (1974)
 Family Education Rights and Privacy Act (1974)
 Rights to Financial Privacy Act (1978)
 Electronic Funds Transfer Act
 Cable TV Privacy Act (1984)
 Electronic Communications Privacy Act (1986)
 Video Privacy Protection Act
 Driver's Privacy Protection Act (1994)
 Children's Online Privacy Protection Act (1998)
 Gramm–Leach–Bliley Act (1999)
 Hospital Privacy Protection Act

concern over privacy, are emerging to identify Web sites that voluntarily agree to follow privacy policies. These approaches rely heavily on the willingness of companies to apply for ratings, to maintain clearly identified policies, and to police themselves. There have been complaints that the seals of approval offered by these agencies are not rigorously enforced.

Two days after the final Data Protection Directive compliance date, United States Secretary of Commerce, William Daley, announced that the EU and the United States would not interrupt data flows, at least for the time being. However, worried about what constitutes an “adequate” level of protection, many influential Americans adopted an alarmist viewpoint about the directive. Information Technology Association president Harris Miller warned that, “This kind of policy could grind the flow of transborder data to a halt ... we urge the Clinton Administration to engage the European Commission and its member states, as well as the business communities on both sides, to engage in an in-depth discussion of the implementation of the directive, its implications upon transborder data flow (TDBF), and, most importantly, already existing practices and policies...”¹⁰

Some writers warned of endangerment to the Organization for Economic Cooperation and Development guidelines, major barriers to world trade,¹¹ or even a trade war.¹⁷ Ohio State University law professor and former chief counselor for privacy in the United States Office of Management and Budget, Peter P. Swire, provided a thorough analysis of how the directive may affect information technology architectures, intranets, extranets, e-mail, the World Wide Web, human resource records, call centers, the financial services sector, medical practices, smart cards, travel reservation systems,

and so on.¹² At the time this article was written, Swire counseled American executives that “a potential way to comply with some of the directive’s requirements is to move data processing operations, and the accompanying jobs, into Europe.”

After two years of discussions with the European Data Privacy Commissioners, the United States Department of Commerce negotiated the Safe Harbor Principles on July 18, 2000. It is posted on the department’s Web site (<http://www.ita.doc.gov/ecom>) and the *Federal Register* (<http://www.access.gpo.gov/nara/cfr/cfr-table-search.html>). Under the Safe Harbor Principles (see Exhibit 2), United States companies can self-certify online that they are fulfilling EU rules on data privacy (<http://Web.ita.doc.gov/safeharbor/shreg.nsf/safeharbor?open-form>). Self-certification needs to be revalidated every 12 months. Among the many firms that have already self-certified are Microsoft Corporation, Hewlett-Packard, and Dun & Bradstreet.

SAFE HARBOR

Over 125 companies, including Intel and Microsoft, have signed Safe Harbor agreements. This refers to a program to be used by firms in countries where personal data processing practices have been deemed inadequate to protect privacy. It was mainly implemented to accommodate the firms in the largest market in the world, the United States. Negotiated by an EC working party and representatives of the FTC in March, 2000, it seeks to reduce the uncertainties of trans-Atlantic data operations so that affected firms will be able to continue their current operations. Safe harbor firms “will then be protected from any arbitrary action by European data protection authorities to cut off data to their companies.”¹³ The seven principles of the Safe Harbor program are notice, choice, onward transfer, security, data integrity, access, and enforcement. Notice indicates that individuals must be notified about how the data will be used. Choice is the ability to opt out or in. Onward transfer extends the information about how the data will be used by transfer to another company. Security restricts the transfer to companies that adhere to the DPPs. Data integrity relates to data accuracy. Data access requires companies to make the data held on an individual is available to that person. Enforcement requires corporate adherence to the DPPs. Some American multinational corporations may find the Safe Harbor principles more burdensome and expensive than doing automatic processing

EXHIBIT 2 Seven Principles of Data Privacy under Safe Harbor

1. **Notice:** In clear language, at the time individuals are asked to provide personal information or as soon thereafter as possible, data processing companies must inform individuals about the purposes for which it collects information, how to contact the organization regarding inquiries or complaints, the types of third parties to which it discloses the information, and the choices available for limiting its use and disclosure.
2. **Choice:** Data processors must offer individuals the opportunity to opt out of data collection, and individuals must receive information on how their personal information is used by or disclosed to third parties. For collecting sensitive information (i.e., medical and health information, racial or ethnic information, political opinions, religious or philosophical beliefs, trade union membership, or sexual information), the individual must give an affirmative or explicit (opt-in) response.
3. **Onward Transfer:** Data processors may only disclose personal information to third parties when this is consistent with the principles of notice and choice.
4. **Security:** Data processors that create, maintain, use, or disseminate must take reasonable measures to ensure the protection of personal information. This includes efforts to protect it from loss, misuse, unauthorized access, disclosure, alteration, and destruction.
5. **Data Integrity:** Data processors may only process personal information relevant to the purposes for which it has been gathered. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is accurate, complete, and current and should avoid secondary uses.
6. **Access:** Individuals must be given reasonable access to data held about them, and they should be able to correct or amend that information if it is inaccurate.
7. **Enforcement:** Mechanisms should be in place to ensure compliance with these principles. This includes methods of recourse for individuals to whom the personally identifiable data. Mechanisms must be available to support affordable mechanisms by which an individual's complaints and disputes can be investigated and resolved and, perhaps, damages awarded. Data processors must have procedures for verifying that the assertions businesses make about their privacy practices are effectively and truly presented. Sanctions must be in place to ensure compliance by the data processor.

directly from subsidiaries in the European countries. Registration for Safe Harbor is with the United States Department of Commerce.

Safe Harbor operations in Europe are not strictly an either-or proposition. The Euro Commission recently authorized transfers of personal data outside the EEA provided such transfers were protected by a Data Transfer Agreement that included (or reassembled) the model clauses published on the EU DP Web site. Like Safe Harbor, these clauses restrict the data importer (usually in the United States) to protect the data to the same level as in Europe. However, it is less burdensome insofar as one can have a data transfer agreement for a particular transfer of a set of data for a particular purpose — whereas Safe Harbor means you have self-certified your entire operation as commensurate with European standards of protection.

Yet, somewhat more flexibility is permitted when data subjects give their informed consent to allow their data to be transferred. However, companies must take action to ensure that the subjects' permissions are not coerced in any way and that permission is freely given with full knowledge of the consequences of their permission.

ISSUES TO BE CONSIDERED

United States and international companies must decide for themselves how seriously they need to take DPP requirements into account. These are some of the issues they should consider.

Data Accuracy

In many countries, IT systems, governmental and private, are not as advanced as they are in Europe and the United States. Nor is there necessarily the will or the money available to bring them to current standards. Hence, for some corporations, data privacy takes a back seat to bringing the systems to the point where they can accurately indicate whether a person is a citizen, is eligible for retirement benefits, or has actually received a warranty for a product purchased.

To Which Standards Should a Company Adhere?

Although the basic principles for DPP are the same in the various countries that have adopted these principles, the precise method for implementing them is not consistent. In France, for example, every database created must be individually approved; while in the United Kingdom compliance is assumed, but the database must be registered. In Germany, the company

Fewer than 150 companies have signed the Safe Harbor Agreement, although this number includes some very large technology companies such as Intel, Microsoft, and Hewlett-Packard.

must have a chief privacy officer who is personally responsible for compliance with the principles. This becomes a problem when companies are international in scope and need to adhere to the requirements of all of the countries.

At some point total adherence becomes impractical. Some privacy authorities say that a company must try its best, be reasonable, and hope that it is within the intent and spirit of the principles to avoid prosecution. Some companies engaged in medical data gathering carefully considered the privacy laws of the EU before settling on the country it believed to have the easiest framework within which to operate.

Which Databases Need to be Approved and Reviewed?

It is not always clear which data are personally identifiable and need to be registered and protected. For example, does the data collected with active badges, GPS localization devices, or wireless telephone location tracking fall into this category? If databases are combined, does the resulting linked database become a new database, thereby requiring a new approval? Generally, all information that is personally identifiable is included: text, images, voice, unique identifiers, and e-mail addresses.

Is Consent Possible?

It is possible that some people whose data is compiled are too old, too young, too sick, or already dead and therefore unable to give permission to have their data shared or used for secondary purposes. Can surrogates give this consent? Since this study is governmentally approved, the question has been raised as to whether legislation supercedes a right of privacy.

Keeping Track of the Laws

The state of data privacy protection continues to unfold, both in the context of the countries that have already adopted this legislation and are modifying the precise techniques in use, as well as in additional countries that are adopting the principles.

Continuing Debate

The rancor between the United States and the EC will probably continue for some time despite the Safe Harbor Principles. Both the United States congress and the EU council of ministers have declared victory on this subject. However, in March, 2001, the Bush administration raised the issue of model contract clauses,

worried that they will become mandatory.¹⁴ In addition, the chairman of the Belgian Privacy Commission, Paul Thomas, recently used the term *e-paternalism* in a discussion of electronic ways to simplify government administration and to denote an attitude of governmental supervision of companies to protect the individual.¹⁵ This is an unfortunate term to be used in the presence of American decision makers who do not feel that the proper role of the government is to provide for the citizens' information technology needs without giving them responsibility. Thus far, fewer than 150 companies have signed the Safe Harbor Agreement, although this number includes some very large technology companies such as Intel, Microsoft, and Hewlett-Packard.

United States Enforcement

Some United States firms and government officials may be under the misapprehension that they can simply self-certify the Safe Harbor Principles with a wink and a nod and then go on operating as they did before. EU officials have stated that lip service to personal data protection is not enough. They expect the FTC to conduct due diligence on these Safe Harbor applications and to enforce the principles vigorously. Registration may be only the first step. In April, 2001, the Department of Commerce announced plans to hire a privacy advisor to monitor compliance and "ensuring that we're not dropping cookies or Web bugs or doing things that people might consider a violation or their privacy."¹⁶ The Department's plans won immediate praise from house majority leader Richard Armey (R-Texas).

Cost of Extending Safe Harbor Principles to Web Sites

According to Robert Hahn, director of the American Enterprise Institute-Brookings Joint Center for Regulatory Studies, the total cost of pending American privacy legislation could be as high as \$36 billion.¹⁷ After consulting with 17 information technology consulting companies, the study concluded that \$100,000 in labor and other costs would be necessary to provide customized software to marketing-active Web sites (About 10 percent of active Web sites or 361,000). This includes the ability for users to access their own personally identifiable information online and correct it as necessary. In addition, the consensus was that off-the-shelf software products would be too difficult to integrate for most Web sites. However, the research

If users, clients, or customers request access to their data, the firm must be able to respond quickly, accurately, and without special effort.

has been criticized by American data privacy expert Peter Swire, who could not come up with a useful estimate himself.

Length of Maintenance

It is not always clear as to how long companies can retain data.

RECOMMENDATIONS FOR UNITED STATES COMPANIES

Secure Top-Level Leadership Recognizing Privacy Protection as an Important Goal

Adherence to the DPP principles is not a simple task, requiring the time and expertise of many people. To the extent that systems must be modified and, perhaps, completely reconstructed, it is also expensive. To do so requires that the president and board understand why there is a need to comply and to understand what adherence demands of the company. Top-level decision makers should also be aware of the privacy concerns of their users, clients, and customers and of the need (and value) to address these concerns.

Appoint a Chief Privacy Information Officer (CPO)

A person with privacy protection responsibilities must be appointed in some countries, but even without this requirement, a company must have someone whose job it is to track privacy law developments, submit approval requests, and communicate with the DPP authorities in appropriate countries. This officer oversees corporate actions aimed at avoiding violations of the laws to which it is subject. The CPO and the compliance committee have especially important roles to play when the company is engaged in a merger with another company that may not have been subject to, but is now subject to, DPP laws.

Establish a DPP Compliance Team

A group of higher-level executives from functional areas across the company should be formed to work with the CPO in order to ensure the infusion of DPP principles across the company. With the CPO, the compliance team would oversee policy setting and the development of corporate policies, initiate training on privacy principles, evaluate privacy issues arising in the business, and ensure that outsourcing contractors are also in compliance. They should also seek to determine what privacy issues are of

concern to their customers and employees and determine whether they can synchronize the company's need for data with the individuals' desires and rights for privacy. Among the policy issues that need to be addressed are those dealing with the identification of disclosure controls, staff training, and the limits on usage of the data by internal staff. The compliance team will also make certain that changes in the DPP rules and regulations are tracked and that changes to local systems are made as needed.

Other issues can arise that require response. If users, clients, or customers request access to their data, the firm must be able to respond quickly, accurately, and without special effort. If a data subject seeks to claim compensation for the misuse of data, it is equally important that the company be able to respond quickly.

Even if a firm exists almost entirely in the United States, it may need to meet DPP standards if it has a Web site that collects data from foreign nationals and, hence, is transferring data from other countries into the United States. Using foreign languages on your site invites the more focused interpretation that you are targeting a particular country or set of countries.

Part of the education of the compliance team may well be attendance at annual meetings of the data privacy protection commissioners who convene once a year to review changes and emerging needs. This public forum enables privacy staff to interrelate and communicate with their peers at other organizations to see how adherence is being structured. Additional information and guidelines can be obtained from such privacy organizations as the Better Business Bureau Online (BBBOnline), TRUSTe, Computer Professionals for Social Responsibility (CPSR), and the like.

Obtain Legal Assistance

The rules and regulations related to the DPP principles vary in their specifics from country to country. They are complex, and your company may well require legal assistance. These rules and regulations change periodically and can be vaguely written; so having a legal expert as a resource is generally required. A small company, in particular, would have an especially difficult time with this task, as would a company involved in particularly sensitive data handling, such as one involved in medical research or in the treatment of patients.

Giving users, clients, and customers the option of having data held on them is a strong possibility if one's intent is to be truly open with them.

Inventory and Audit Databases with Personally Identifiable Data

Many companies are not aware of how much data is collected, how and by whom it is being used, and whether this data collection is consistent with corporate policy and corporate mission. Neither is it always known whether persons without authorization have access to the data held in these databases. Audits of security measures should be undertaken as well to ensure that only authorized persons operate in accordance with the DPP principles and under nondisclosure policies. Companies will have to examine data centers in multiple settings to see that their data contents, data processing, and transfer procedures are not in violation of the DPP principles. Remember that the databases in question include personnel as well as customer and client databases.

Ensure adequate security. The DPP principles hold liabilities not just for willful disclosure but also for unauthorized data releases. Systems should be designed for secure internal staff access and for the prevention of incursions by hackers and people who lack authorization.

As new systems are developed, the CPO of the firm should ensure that all users of corporate data have input into ethical and legal characteristics of the systems. Think through design requirements and specifications to ensure that the highest levels of security and protection exist.

Another issue to be addressed is that of opt-out and opt-in choices. Giving users, clients, and customers the option of having data held on them is a strong possibility if one's intent is to be truly open with them. If this is the case, make it clear that this is an option and make it equally clear how one can opt out entirely or simply withhold some unneeded data.

Naturally, there exists the possibility that some of your practices are in violation of the DPP principles. If so, implement changes immediately to bring your data collection, manipulation and transfer policies into alignment with the principles.

Recognize that Privacy Regulations Are Not an Excuse Not to Collect Data

It is true, of course, that the data privacy protection requirements impose work on the companies that collect such data. Clearly, one cannot simply assert that a company cannot collect personal data. The requirements do not eliminate the possibility of doing so. They do force the company to make a conscious decision as to whether they have a need to collect the

data and then to identify means of informing the individuals involved as to their rights.

Focus on Consent

In many respects, the end result of the DPP principles turns out to be little different in the EU than it is in the United States. Much data is still collected and used, for instance, for marketing purposes. The greater visible difference is the emphasis that DPP-adherent countries place on informed consent. Their companies cannot be so secretive in their operations that the alert consumer would not know what permissions they are transferring to the companies with the divulgence of personal data.

Be Aware that A Web Privacy Policy Does Not Adequately Address the DPP Principles

Such a policy may go part of the way to establishing whether your company qualifies under the principles or under Safe Harbor provisions; but in and of itself, it is not necessarily sufficient either to fully inform users of their options or to satisfy the requirements for DPP compliance. Many media must be addressed to ensure that all affected parties are aware of and, hopefully, in support of the privacy policies in place.

Consider Applying under the Safe Harbor Provisions

A company engaged in processing data in a DPP country might choose to sign the Safe Harbor agreement. Other alternatives exist. One alternative is contracting with a company in that country to collect and process the data. This is facilitated by the development of model contractual agreements to guide such collections and processing. Another strategic move is actually moving a data center into the EU since it is easier to move data out of the EU than it is to move it in from the United States. Yet another alternative is running one set of data systems in DPP countries and another in the United States.

Consider Implementing P3P on Your Web Sites

The Platform for Privacy Practices (P3P) is an emerging XML standard, which automates the exchange of data between a site and its visitors. Users of P3P are able to indicate to their browser which data they choose to share as they visit Web sites. Sites requesting this data receive the

data automatically as the user moves onto the site.

It is incumbent upon IT managers to make sure that corporate executives understand the differences between United States and European (and other national) perspectives and laws.

Keep Abreast of Emerging Issues

New technologies introduce new opportunities for both business improvements and public-relations disasters. As new hardware and software technologies are considered for implementation, the privacy team must determine whether new policies are needed and whether it should take actions to avoid the collection and misuse of data. This is especially true when the technologies are or could be used for employee and activity surveillance. In this respect, technologies such as XML, processor and IP address checking, new browsers, and wearable processing chips come to mind.

SUMMARY

The DPPs and the laws guiding their implementation are not a transitory phenomenon. As soon as a company is engaged in international data practices, it becomes subject to the laws implementing the principles. It is incumbent upon IT managers to make sure that corporate executives understand the differences between United States and European (and other national) perspectives and laws. As the CPO of Experian Corporation observed, "Compliance is not a cost to the business, but a legitimate cost of doing business." ▲

References

1. Gentot, Michel (April 2001). *J. 23rd Intl. Conf. Data Prot. Commissioners*. France: Commission Nationale de L'Informatique et des Libertés. No. 2., p. 1.
2. Simitis, S. (1995). From the market to the polis: the EU data protection directive on the protection of personal data. *Iowa Law Rev.* 80(3), pp. 445-469.
3. Smith, Kent A. and Patricia E. Healy. Abstract from transborder data flows: the transfer of medical and other scientific information by the United States. *Inf. Soc.* 5(2). Accessed on 7/12/2001. <http://www.slis.indiana.edu/TIS/abstracts/ab05-2/smith.html>.
4. Klosek, Jacqueline (2000). *Data Privacy in the Information Age*. Westport CT: Quorum Books. Chapter 4, pp. 51-127
5. Ward, Mark (July 11, 2001). The Problems of Protecting Privacy. BBC News Online. Accessed on 8/29/01.
6. Trading in Information. BBC News Online. Accessed on 8/29/01. http://news.bbc.co.uk/hi/english/sci/tech/newsid_1434000/1434131.stm.
7. Medical Research In Peril. BBC News Online. Accessed on 8/29/01. http://news.bbc.co.uk/hi/english/health/newsid_1323000/1323256.stm.
8. Remarks of Secretary of Commerce William M. Daley, February 5, 1999. <http://204.193.246.62/public.nsf/docs/commerce-ftc-online-shopping-briefing>. Cited from Klosek, Jacqueline (2000). *Data Privacy in the Information Age*. Westport CT: Quorum Books. p. 2.
9. Deans, C.P., Karwan, K.R., Goslar, M.D., Ricks, D.A. and Toyne, B. Key (1991) International IS issues in the U.S.-based multinational corporations, *J. Manage. Inf. Syst.*, 7, 4 (1991), 27-50. Accessed on August 28, 2001. <http://www.terry.uga.edu/mis/iris/usmnc.html>.
10. *Business Wire* (October 24, 1997).
11. Vastine, Robert (July 30, 1997). Battling over data privacy. *J. Commerce*.
12. Swire, Peter P. and Robert E. Litan (October 21, 1997). None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive. Interim report issued for a conference of the Brookings Institution. Accessed on August 28, 2001. <http://www.acs.ohio-state.edu/units/law/swire1/noyb.htm>. Note: Some information provided may have been superceded under the Safe Harbor Principles.
13. David Aaron, Undersecretary of Commerce for International Trade. Cited from Thibodeau, Patrick (March 20, 2000). Europe and U.S. agree on data rules. *Computerworld*. Framingham. Accessed on 2/1/01. <http://proquest.umi.com/>.
14. U.S. raises issues with EU over data privacy laws. (March 28, 2001). *Reuters*. Accessed on 4/16/01. <http://news.excite.com/news/r/010328/11/eu-us-privacy>.
15. Thomas, Paul (July 2001). *J. 23rd Intl. Conf. Data Prot. Commissioners*. France: Commission Nationale de L'Informatique et des Libertés. No. 3., p. 1.
16. Thibodeau, Patrick (May 1, 2001). Senators call for addition of federal CIO." *Computerworld*. Quote is from a Commerce Department spokesman. Accessed on 8/28/01. www.computerworld.com/cwi/story/0,1199,NAV47_STO60120,00.html.
17. Johnston, Margret (May 14, 2001). Study: Privacy Proposals Could Cost Billions. IDG. Accessed from CNN.com on 8/28/01. www.cnn.com/2001/TECH/industry/05/14/costly.privacy.proposals.idg/index.html.

