EMERGING TRENDS IN INTERNATIONAL PRIVACY LAW

15 Emory Int'l. L. Rev. 87 (2001)

Jeffrey B. Ritter, Benjamin S. Hayes, Henry L. Judy

Introduction

As information technology continues to develop rapidly, increased opportunities and incentives are created to collect data on individuals and use that personal data for diverse and lucrative purposes. Some believe that in a global information economy, perhaps the most valuable electronic asset will be aggregations of information on individuals. For over two decades, concerns regarding the privacy of the individual have been reflected in significant European legal governance on the collection and cross-border movement of personal data. In recent years, these concerns have escalated in Europe and in other economies, particularly due to the rapid commercialization of the Internet and the development of new and more powerful information technologies. These concerns have motivated an accumulation of privacy law, with recent enactments in the United States, Europe, and other areas of the world. (footnote omitted)

Across the emerging body of global privacy law, which varies substantially from jurisdiction to jurisdiction, general patterns are beginning to emerge. In general, virtually every piece of information related to an individual is defined as "personal data," and therefore potentially subject to regulation with respect to its collection, processing, use, and transfer. Different elements, types, and uses of personal data are subject to different levels of regulation. Typically, the collection and use of medical and other highly sensitive data--such as data revealing the subject's race, religion, political affiliation, or sexual orientation, or data relating to children--is most highly regulated.

What conduct is regulated? Privacy laws are structured on the essential principle that the individual person--a "data subject"--should retain control over the information about himself or herself that is collected or used by anyone, whether in business or government. Privacy laws impose obligations that are intended to prevent the collection or use of information in any manner that is inconsistent with the expectations of the data subject. In effect, the data subjects' control of their own personal data cannot be circumvented or denied except with their consent. Essentially, each time personal data is collected, a contract is established with the data subject that governs the onward use of that personal data. Privacy laws empower the data subject and the state to enforce the data subject's rights under that agreement.

Privacy laws are both simple and complex. Their simplicity is found in the fact that, across different legal systems and, particularly in the United States, across different regulatory schemes governing different industries, the applicable statutes and regulations embrace comparable core principles, also referred to as "fair information practices." (footnote omitted) The complexity is found in the reality that different sovereign nations have embraced different political and social objectives in their regulation of privacy. As a result, the regulation of privacy in the year 2000 brings escalated political rhetoric regarding the use or misuse of personal information in the creation or extension of trade barriers. Recent protracted and difficult negotiations between the United States and Europe have been representative of the challenging diplomatic dimensions.

For chief information officers, security officers, general counsels, systems designers, and consultants of any company charged with assuring compliance with privacy laws, the rules of the game are changing. The accelerated emergence of regulatory controls that target information assets with significant economic value is transforming how information systems are designed and managed. Technology executives are required to assume increased responsibility for legal compliance across divergent legal regimes. Business executives and legal officers are required to acquire significant new understandings of the technologies deployed in information management and the business relationships through which personal data is

collected, used, and transferred in support of the execution of business relationships.

What makes privacy law important to all of these participants is not the imposition of yet another set of regulations requiring compliance. Instead, privacy law tests companies in their ability to truly integrate business, law, and technology into the coherent planning and execution of their information systems. Few question the value of the Y2K exercise in advancing companies and their business partners to a new level of interdependent collaboration. Privacy presents the next threshold. As the world's economy continues its remarkable transformation into a global environment in which information in electronic form is a significant measure of economic wealth, we believe those companies that master privacy as a competitive opportunity, rather than as a regulatory cost without economic benefit, will be best positioned to remain competitive.

This Article introduces the evolution of privacy law to the point at which it stands today and endeavors to provide perspectives on the principles and trends that are emerging from the laws and regulations currently in effect. This Article presents three distinct, but overlapping, models for managing the collection and use of personal data. What makes the management of personal data different is the degree to which, in managing compliance, the use of contracts and other legal tools becomes indispensable to the creation of solutions providing competitive advantage.

I. The Evolution of Privacy Law

* * *

B. The European Directive on Data Protection

The challenges of achieving efficient information flow came to the attention of Europeans seeking to engineer the emergence of today's European Union. The disorder under the earlier transborder data flow laws was recognized to be significantly disruptive to the objective of achieving an "open" internal market among the European nations. Thus, in 1990, in an effort to both (1) ensure that member states protected "fundamental" privacy rights when processing personal data, regardless of the national citizenship of the data subjects, and (2) prevent member states from restricting the free flow of personal data within the European Union, the European Commission proposed the E.U. Directive on Data Protection. On October 24, 1995, following years of discussion and debate, the Council and Parliament of the European Union adopted the final version of Directive 95/46/EC ("E.U. Directive" or "Directive"). (footnote omitted) The Directive became effective on October 25, 1998.

The Directive generally embraces the same essential "fair information principles" that had characterized the COE Convention and the OECD Guidelines. The requirements are compared to other national laws in Section II (B); (footnote omitted) but several important aspects of the Directive deserve to be emphasized:

•The Directive adopts a generic architecture toward personal information that does not create special rules based on the industry in which those collecting or processing the data are engaged. By contrast, the Directive endorses the principle that the nature of the data, not its use, determines the rules that will apply.

•The Directive does not eliminate national diversity in regulation. Any European Union directive pursues harmonization among the member states by defining minimum standards around which each member state must enact enabling legislation. (footnote omitted) The Data Protection Directive affords member states a "margin for manoeuvre," (footnote omitted) although they must enact laws at least as restrictive as the Directive. As a result, European nations have not enacted identical laws, nor have they implemented consistent regulatory processes. (footnote omitted)

•The Directive extends restrictions on transborder data flows to govern any export of personal data to non-European destinations. The Directive presumes that transfers among European countries occur between nations with acceptable harmonized laws. However, with respect to transfers of personal data to non- E.U. countries, Article 25, Paragraph 1 of the E.U. Directive sets forth the standard that "the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if . . . the third country in question ensures an adequate level of protection." (footnote omitted)

•The Directive imposes significant procedural requirements on the collection or use of sensitive data or data intended for use in direct marketing to consumers. Essentially, the data subject involved must affirmatively take action that produces a record of their "unambiguous consent" to the collection or use of personal data in those circumstances. At the least, in some circumstances, an "opt-out" by the data subject is acceptable. However, the E.U. Directive definitively advances the principle that the collection or use of data must be accompanied by the creation of suitable records evidencing the "contract" accepted by the data subject.

C. United States Law

The legal architecture in the United States for the protection of personal data is structured entirely differently than in Europe. In the United States, requirements for the collection or disclosure of personal information have been enacted to respond to particular pressures in particular industries. This sectoral approach is in significant contrast to the European generic architecture. The result is that the same types of personal information may be subject to different regulatory controls. Distinctions are made between industries (e.g., financial services, health services, video rentals), data sources (e.g., children), and the sector of society in which the information is collected or used (public sector or private sector). In addition, the various states of the United States are empowered to enact laws governing privacy with respect to the activities of individuals and companies located within their borders and with respect to persons located outside their borders whose activities with respect to data produce the jurisdictionally requisite effects within their borders. Virtually hundreds of independent laws have been placed into effect that amplify, at the state level, the sectoral approach, producing regulations that often present challenges to companies similar to those in Europe.

Several examples of federal law illustrate the sectoral, data-specific facets of American law:

•The Gramm-Leach-Bliley Act (GLB), enacted in 1999, requires every financial institution to protect the security and confidentiality of its customers' nonpublic personal information, disclose its privacy policies to consumers, and provide consumers with an opportunity to direct that the institution not share their nonpublic personal information with unaffiliated third parties. (footnote omitted) Violations of the privacy provisions of GLB are subject to enforcement by various federal regulators; the specific sanctions that may be imposed vary according to the regulatory agency that has jurisdiction in a particular case.

•The Fair Credit Reporting Act (FCRA) governs the activities of consumer reporting agencies and protects the privacy of consumers' credit information by limiting the circumstances under which a consumer reporting agency can disclose a consumer report. (footnote omitted) Failure to comply with FCRA constitutes an unfair or deceptive act or practice under the Federal Trade Commission Act, and can result in damages, civil penalties, and, in some cases, criminal liability.

•The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates the establishment of standards to protect the privacy and confidentiality of individually identifiable health information. (footnote omitted) Under HIPAA, the Department of Health and Human Services has proposed rules, not yet effective, to implement the legislative mandate. (footnote omitted) Both civil and criminal penalties can be assessed for violations.

•The Children's Online Privacy Protection Act of 1998 (COPPA) prohibits the collection, use, or disclosure of personally identifiable information from and about children under the age of thirteen on the Internet without prior "verifiable parental consent." (footnote omitted) Violations of the COPPA are enforced as "unfair or deceptive" trade practices by the Federal Trade Commission. (footnote omitted)

One of the distinct characteristics of U.S. law is that the regulations focus entirely upon domestic operations and activities. In stark contrast to the European architecture, which generally presumes personal data will move across borders, U.S. law is particularly insensitive to this dimension of the emerging global economy. In addition, in the absence of mandatory preemption of the jurisdiction of the state governments to regulate privacy, the ability of the states to introduce legal requirements that may affect international data transfers remains potent. The federal government, except in the specific sectors regulated by federal law, has not chosen to preempt the power of the states to regulate privacy.

Another aspect of the U.S. legal approach is the extended degree to which Congress delegates the responsibility for developing implementing regulations consistent with enacted legislation to administrative agencies. This concept is not new to electronic commerce; however, for many aspects of electronic commercial practices, the scope of the delegation is important. Enacting suitable regulations often involves examining various technologies and making choices that inevitably influence the direction of electronic commercial practices. (footnote omitted) As a result, the law extends beyond technology-neutral policies; specific technologies can be mandated into commercial practice. Moreover, different industries can adopt different technology architectures for executing comparable transactions. Since many companies operate concurrently in different industries, the administrative laws can place stress upon the normal business objectives of achieving uniformity and consistency in information technology systems.

D. The Developing Conflict--Politics and Privacy

The difference in approaches between the European Union and the United States has escalated into international political focus. Until the 1998 effective date of the Directive approached, the requirement of the E.U. Directive restricting the export of personal information only to other nations with laws offering adequate protection (footnote omitted) failed to capture significant attention in the United States. But, since no official body in either the European Union or any individual European nation had determined U.S. law to be "adequate," ongoing data transfers from Europe to the United States across a wide number of significant industries (airlines, entertainment, credit cards, retailing) were in jeopardy of being disrupted. American companies claimed that the E.U. Directive represented an enormous non-tariff trade barrier, suddenly placing essential businesses and services of mutual benefit to both economies at risk. Europeans defended the export restrictions on the grounds of (a) protecting the interests of European citizens against exploitation of their data by U.S. interests, and (b) encouraging European data sources to find European providers of the kinds of services otherwise being sought in the United States (thereby facilitating economic growth of the internal market of Europe).

In April 1998, the United States and European Commission officials entered into negotiations that would create a "safe harbor" for American companies desiring to export from Europe personal data relating to European citizens. The objective was to establish a mechanism through which American companies (and their trading counterparts) would not be required to prove the adequacy of American law as a condition to the execution of data transfers. Critical to the Europeans was assuring that both European governments and individual citizens would be able to enforce their rights under the E.U. Directive in the event their personal data was misused or otherwise abused.

Despite enormous commitments of resources, and the significant involvement of private sector interests in supporting the analyses and negotiations between the governments, the Safe Harbor deliberations were slow to produce results. The Europeans endeavored to achieve two important goals: the agreement of

American companies to the jurisdiction of European authorities or, in the alternative, the pre-approval by European officials of the terms of any commercial agreements under which data transfers toward the United States would be executed. (footnote omitted)

Difficult negotiations ultimately produced a formulation under which European negotiators would recommend that transfers of personal data from the European Union to the United States be allowed for those companies willing to comply with proposed "Safe Harbor Principles." Negotiations began in April 1998, and the Department of Commerce has proposed five drafts of the Safe Harbor Principles. The Department issued its final draft on July 21, 2000. (footnote omitted) Under those Principles, in the absence of committing to the jurisdiction of European officials, an American company exporting personal data on European citizens may:

•Self-certify, on a voluntary basis, with the United States Department of Commerce its adherence to principles for the protection of personal data that are consistent with European legal principles, which adherence must be publicly announced; or

•Join a self-regulatory privacy program that adheres to the Safe Harbor Principles, thereby qualifying the company for the Safe Harbor. Examples such as TRUSTe or BBBOnline have been cited as representative of the types of programs contemplated. (footnote omitted) In effect, the government is furthering self- regulation by deferring to non-government programs to enforce suitable standards on participating companies.

Companies subject to explicit federal regulations regarding the privacy of personal information (such as HIPAA or COPPA) (footnote omitted) may also be eligible to self-certify their compliance with the applicable laws and gain the Safe Harbor recognition that would permit their transactions with European data to occur. (footnote omitted) In any case, the failure of a company to adhere to its announced commitment has been declared actionable under the United States Federal Trade Commission Act prohibiting unfair and deceptive acts. (footnote omitted) In addition, companies would be subject to sanctions under other applicable laws. (footnote omitted)

Article 31 of the Directive establishes a committee that is the first body to review any international agreement for adequacy in regard to the Directive. At its May 2000 meeting, the Article 31 committee endorsed (after having previously refused to do so) the latest draft of the Safe Harbor Principles. Following this recommendation, the European Parliament adopted a resolution denouncing the Safe Harbor and recommending that the arrangement not be adopted. (footnote omitted) The Parliament stopped short, however, of making a determination that the Commission (represented by the Article 31 Committee) had exceeded its authority in negotiating and endorsing the Safe Harbor. The Commission chose to ignore the criticism of the Parliament and on July 28, 2000 issued its final determination that the Safe Harbor Principles were adequate, clearing the way for the arrangement to be implemented. (footnote omitted)

In the United States, the actions of the Department of Commerce have drawn criticism from several major international companies who have indicated continued dissatisfaction with the final proposal. (footnote omitted) Presently, European officials in those nations that have enacted laws responsive to the E.U. Directive are authorized to enforce those laws against American companies or their trading partners involved in exporting personal data. To date, no conspicuous actions have been taken (largely as a result of an informal "stand-still" agreed upon during the pendency of the Safe Harbor negotiations). (footnote omitted)

The conflicts between Europe and the United States are illustrative of the larger dimensions of a growing body of international privacy law. Jurisdictional variations--whether among regions, among nations, among states or among combinations of any of them--ultimately conflict with any enterprise's business

objectives to design and operate consistent information management systems with uniformity in standards, operations and processes whenever possible. Both Europe and the United States have proceeded in good faith, within their own unique cultures, economies and politics, to protect the privacy of citizens in the collection and use of their personal information. However, as systems increasingly operate without regard to geographic considerations, the political conflicts place at risk enormous economic investments. These conflicts are not limited to privacy law; exactly the same phenomenon is presented by issues of biosafety regulation, food labeling, the responsibility of Internet Service Providers for the content they carry, and a host of other issues that do not immediately appear to be related.

Changes in privacy laws can cost companies millions of dollars, euros, or yen in establishing different operations to comply with different local legal rules. Economic competition among governments and regions can interfere with effective systems designs that meaningfully manage personal information through a variety of technology and process architectures. Inconsistent regulations of different sectors in which many companies may concurrently conduct business can make the benefits of integrated operations more difficult to achieve. The regulation of privacy is gaining influence as a potentially significant disruptive force in the planning and operation of sound information technology practices.

E. The Rest of the World's Legal Reforms

While Europe and the United States struggled to achieve consensus on the Safe Harbor proposals, the rest of the world has not been ignoring the privacy issue. Indeed, the political implications of the debates have influenced other nations to proceed toward enacting privacy legislation which, based on consultations with officials of the European Commission, would meet the adequacy standard of the E.U. Directive. For those countries, achieving alignment with the European Union on the privacy issue has been considered an important bridge toward increased economic opportunities with the lucrative European marketplace. In addition, in many nations in which there is less conflict between the public and private sectors (as compared to the U.S. political environment), the enactment of a generic architecture for privacy law is significantly easier to accomplish.

Additionally, rights of privacy have been granted in a number of countries' constitutions in order to remedy past abuses. Examples include Hungary, (footnote omitted) South Africa, (footnote omitted) and Lithuania. (footnote omitted)

Legislation has been enacted in several nations with common law traditions, notably Hong Kong, (footnote omitted) New Zealand, (footnote omitted) and Canada. (footnote omitted) Proposals are pending in other countries. The enacted laws are remarkably similar in their embrace of European fair information principles. In this respect, the European Union is observing the successful exportation of its view of effective privacy regulation. In some ways, this may not be a desirable result, as some advocates for the E.U. Directive gave great weight to the favoritism within the Directive for intra-European data transfer activities. Nonetheless, the early trend is for others to simply mimic the European regulatory framework and, in so doing, to create a path toward a finding of adequate protection that will allow for ongoing and future data processing without disruption.

For companies doing business beyond Europe and the United States, the potential for inconsistent legal architectures exacerbating current inconsistencies in the law actually appears fairly modest. The European framework is proving to be both politically appealing and, for nations concerned that the global dimensions of the Internet will marginalize the continued role of governments in trade regulation, is providing a renewal of public purpose. Indeed, driven by an appetite for avoiding alternative legal frameworks, multinational companies, particularly those originating in Europe and more familiar with privacy compliance as a routine part of doing business, are not vigorously opposing the exportation of the European legislative model.

F. Certain Current Events

In addition to the pending status of the implementation of the Safe Harbor Principles proposed by the United States Department of Commerce, other dimensions of ongoing privacy law reforms in the United States are important to highlight. Consistent with earlier observations, American businesses are discovering that designing a path forward for managing personal information cannot be reliably executed merely because Congress has enacted federal legislation. For instance, despite the enactment of GLB, delayed implementation of its regulations, proposed additional federal legislation, and a proliferation of state legislation have created great uncertainty for financial institutions in choosing a path forward.

1. Delay in Gramm-Leach-Bliley Implementation

Following the enactment of GLB, the Clinton Administration lobbied Congress to enact new legislation tightening the control consumers have over their personal data given to financial institutions. Nonetheless, the final regulations implementing the Gramm-Leach-Bliley privacy provisions pushed back the date of implementation by seven months, coming into force on July 1, 2001. The regulations still purported to become effective on the original implementation date, November 13, 2000, but compliance was voluntary until the later date. The Clinton Administration's position in favor of stricter controls clearly undermined arguments that GLB is adequate from a European perspective. (footnote omitted)

2. Federal Trade Commission

The Federal Trade Commission (FTC) is responsible for enforcing consumer protection laws in the United States and taking action against unfair or deceptive trade practices. The FTC has determined that the mismanagement or misuse of personal information, when in conflict with a company's announced privacy policies, constitutes potentially deceptive trade practices against which the FTC may take enforcement action. (footnote omitted) Though the FTC has until recently encouraged industry to establish and maintain suitable self-regulatory privacy protections, on May 23, 2000, the FTC released a report, Privacy Online: Fair Information Practices in the Electronic Marketplace, calling for federal legislation to impose extensive privacy requirements on businesses in multiple industry sectors. (footnote omitted)

3. Activity in U.S. State Legislatures

In the past three years there has been an explosion of legislative proposals on the state level dealing with every aspect of privacy protection. Legislative proposals dealing with privacy issues are currently pending in approximately 80% of state legislatures. Indeed, since Congress enacted the Gramm-Leach-Bliley Act in November 1999, numerous state legislatures have introduced financial privacy legislation that, if enacted, would provide consumers with stronger privacy protections than the Act. This is possible since the Gramm-Leach-Bliley Act does not preempt state privacy provisions that are more protective to consumers than its provisions. Many of these state proposals would:

•Require that consumers opt in before financial institutions could share their personal information with third parties;

•Contain restrictions on the sharing of consumers' personal information among affiliates;

•Restrict the circumstances under which financial institutions could use consumers' personal information for marketing the institution's own products and services; or

•Prohibit financial institutions from requiring their customers to disclose any information that is not necessary in connection with the product or service the consumer desires to obtain from the institution.

Some recent state privacy proposals would also affect broader segments of commercial activities than simply "financial services." Examples of such proposals include:

•A bill in New York State would require the affirmative written consent of data subjects before any personal information could be transferred to any entity, whether affiliated or not.

•In Arizona, a proposal would limit the gathering of personal information to only that which is "reasonably necessary to perform the transaction." All other personal information requested would have to be marked as "optional."

•In California, any entity offering direct access to the Internet (which may include businesses that provide employees with dial-up Internet access) would have to offer notice and choice before any transfer of personal information, under a proposed law in that state.

•In Michigan, two proposed laws would prohibit both the transfer of any personal information without prior consent and the conditioning of any transaction on the granting of such consent.

•A proposed law in Hawaii would prohibit any collection or transfer of personal information without the consent of the data subject, subject to certain restrictions. This proposed statute, in a state that is a crossroads for international trade in the Pacific, specifically references the E.U. Directive, the Hong Kong Ordinance, and the New Zealand privacy law as providing the impetus for its passage. In doing so, the legislation underscores the potential for state governments to be involved in international trade policy aspects of privacy.

The significance of this activity on the state level is highlighted by the fact that trade associations representing significant elements of the U.S. financial services sector took the position that they were unwilling to consider supporting the legislation that was advanced by the Clinton Administration unless federal preemption of state privacy laws was "on the table." In the absence of such preemption, U.S. federal law would be merely a floor for state legislation. If such preemption were adopted, significant advantages of legal consistency and reduction in compliance costs within the U.S. internal market would be achieved. However, privacy activists strongly oppose such a preemptive regime.

G. The Concept of Self-Regulation

A significant source of the momentum for the growth of the Internet has been a political commitment, particularly in the United States, to promote self-regulation as an effective strategy for responding to the concerns that often motivate the enactment of new laws. In July 1997, then-President Clinton announced a Framework for Global Electronic Commerce that committed his Administration toward a policy of self-regulation. (footnote omitted) Privacy has been one of the few policy areas in which industry initiatives have achieved momentum, though their success in diverting new legislation is apparently minimal.

TRUSTe and BBBOnline are the self-regulatory programs of two nonprofit organizations. (footnote omitted) TRUSTe was launched from within the Internet, sponsored by the Electronic Frontier Foundation; the second program is grounded in the self-regulatory efforts of a traditional organization, the Better Business Bureau. Each program offers companies, particularly those conducting business on the Internet, the opportunity to register their compliance with described privacy practices and to agree to certain investigation and enforcement processes. For example, both programs establish qualifying criteria for privacy policies to be used by Internet-based businesses. Both programs promote practices that are consistent with the emerging principles of privacy law (as discussed in Part II).

There are two important characteristics to these self-regulatory programs. First, qualifying registered companies are permitted to display on their websites the logo or icon of the program. This logo is intended to communicate to consumers a "seal of approval" of that company's privacy practices. Second, enforcement of the privacy standards occurs through organizational sanctions only. There is no recourse to traditional venues, such as the courts, in the event of non-compliance. The TRUSTe program has been influential in causing the Safe Harbor Principles to identify and endorse self-regulatory programs as a compliance strategy. However, practical success has been mixed. On more than one occasion, companies that have purportedly violated their privacy policies have refused to implement changes mandated by TRUSTe.

In July 2000, a group representing ninety percent of Internet advertising companies formed the Network Advertising Initiative (NAI). The NAI was chiefly a response to a privacy controversy that severely impacted the stock price of leading Internet advertising company Doubleclick. The controversy surrounded a Doubleclick plan to merge vast amounts of non-personally identifiable data collected about the web surfing habits of millions of Internet users with the personally-identifiable profiles of these users' offline purchasing habits, amassed by Abacus Direct, a market research company, and acquired by Doubleclick in 1999. Doubleclick developed this plan in spite of an earlier promise that no such combination would occur. Following an outpouring of consumer complaints, as well as the threat of investigations and suits by the FTC and several states, Doubleclick abandoned the plan, although it reserved the right to revisit it in the future.

The NAI is a self-regulatory initiative for the Internet advertising industry that establishes basic rules of conduct, including that non-personally identifiable information may be merged with personally identifiable information only with the express consent ("opt-in") of the data subject. The Clinton Administration applauded the NAI as a positive step toward effective self- regulation, but indicated that it still favored legislation to underpin the initiative and bring those companies that have not joined the NAI into compliance with its principles. (footnote omitted)

H. Conclusion

In supporting the Safe Harbor Principles, the United States Department of Commerce has argued that existing law in the United States, together with the processes described in the Safe Harbor materials, provides adequate protection regarding personal information. But, taken as a whole, the continued introduction or proposal of additional legislation in the United States significantly undermines the credibility of the Commerce Department's position. The political appeal in a democratic environment for proposing privacy legislation cannot be discounted; nevertheless, the sectoral approach of American lawmaking continues to define new privacy proposals. Few proposals in the United States commit to the formulation of a generic architecture for privacy regulation comparable to that established by the E.U. Directive.

The result is significant instability in the legal landscape while, at the same time, more and more enacted laws or regulations move toward or beyond their effective date. Companies doing business in personal information face considerable risk in crafting responsive systems and business practices. Those businesses not implementing compliant practices, based on the laws currently in effect, face possible prosecution or civil actions. But, for many, the instability of the legal landscape makes significant infrastructure investments toward privacy compliance difficult to justify in the absence of a better sense of the governing standards. As one executive has privately observed: "We don't really care what the rules are; we just need to know what the rules are in order to commit our resources."

II. Core Principles of Privacy Law

Though there exists significant instability in the legal framework of privacy laws, certain substantive principles are emerging that are generally common to any legislative solution. (We distinguish "substantive" principles from "process" issues like compliance, which is addressed in Part III below.) These substantive principles find their origins in the structures of the COE Convention and the OECD Guidelines and are certainly reflected in the details of the E.U. Directive and the Safe Harbor Principles of the U.S. Department of Commerce. At the same time, many of the current U.S. and non-European legislative proposals are also reflective of these principles, often to a far greater degree than in privacy legislation enacted prior to the effective date of the E.U. Directive.

The emergence of these core principles is vitally important to any company seeking to engineer improved personal information management processes and systems. By targeting the implementation of processes that are consistent with the core principles, companies can best position themselves within their own form of safe harbor. In the event of new legislative or regulatory changes, a company that has committed to this Safe Harbor is positioned to implement conforming practices more efficiently than others. In the long run, competitive advantage will likely be realized by those most capable of implementing in the marketplace the first solutions responsive to new regulatory mandates.

The interdependent nature of an information economy increases the potential advantages of that leadership. No law will completely prescribe the exact formulation of compliant practices; indeed, despite some instances in which agencies must endorse particular technology solutions, most agencies, particularly in the United States, favor technology-neutral frameworks that allow regulated entities the flexibility to craft their own solutions. Thus, those companies that show leadership in building privacy management practices based on the core principles are likely going to be able to first offer solutions for adoption by others. This allows them to also be able to avoid being asked by multiple business partners or competitors to adopt other alternatives, again providing greater operating efficiencies.

The core principles emphasize the contract-based nature of privacy regulation. Under both common and civil law systems, a contract consists of an offer and an acceptance. What becomes readily apparent in reviewing the core principles is that, in operation, they function to assure that each party to the collection or use of information takes certain actions that represent essentially a series of offers and acceptances. Thus, the regulation of personal information can be re-evaluated as a specialized subset of contract law. In that context, information systems can then be designed and managed more along traditional business processes. What is different is that the asset of the deal is the personal information of the data subject. In all other respects, however, creating and retaining suitable business records to demonstrate the existence of proper contracting arrangements is very comparable.

A. The Core Principles

What, then, are the core principles? The following core principles are supplemented by a chart which illustrates, across a few leading jurisdictions and one self-regulatory program, how each principle is reflected in the enacted law or operating rules.

•Notice: Under the Notice principle, organizations provide individuals with a notice describing the types of personal information the organization collects, the purposes for which the organization collects and uses such information, the types of third parties to which the organization discloses such information, the choices the organization offers individuals for limiting information use and disclosure, how individuals may access their data, if they may, and the organization's contact information. A suitable notice represents, in effect, an offer of the terms on which the personal information may be collected and used.

•Choice: Under the Choice principle, organizations offer individuals choice regarding certain uses of their personal information, or the disclosures of their information to third parties, under certain circumstances. Typically there are stricter rules for "sensitive" information, mandating that (except under

certain specified circumstances) individuals must give explicit, unambiguous consent before their information may be used or disclosed. Suitable choice is all about providing an acceptance, tailored to the nature of the data and proposed uses, of the offer presented by the notice. The more sensitive the data, or the greater the potential for misuse or abuse of that information, the stronger the requirements for how choice must be evidenced.

•Onward Transfer: Under the Onward Transfer principle, an organization is permitted to execute an onward transfer of personal information to third parties only in a manner that is consistent with the notice and choice provided at the time the information was collected. This principle places an obligation on organizations to establish controls on both (a) the third parties to whom any personal data is transferred, and (b) the uses of the personal information made by those third parties. These controls may be established both by technologies and by private contracts, such as data transfer agreements. These agreements extend the contract-based architecture; an offer and an acceptance condition and regulate the information in order that the transfer participants comply with both the offer contained in the original notice, together with other requirements that may be established by applicable law.

•Security: Under the Security principle, organizations are required to take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration, and destruction. Implementation of the Security principle occurs at each stage of the lifecycle of personal information. Those collecting and processing the personal data must design and manage security commensurate with the sensitivity or value of the information, both to the data subjects and to their respective businesses.

•Consistency: Under the Consistency principle, an organization does not process personal information inconsistently with the announced purposes for which it was collected. Those processing information may introduce new uses, but must provide notice and effective choice to the data subject before doing so. To the extent necessary, organizations take reasonable steps to ensure that collected personal data is relevant for its intended use, accurate, complete, and current. Under this principle, careful attention is given to the scope of the notice given (i.e., the basis of the bargain) in order to balance the need for full and fair disclosure to the data subject with any potential and unforeseen uses of the data that an organization may later wish to make.

•Access: Under the Access principle, individuals are given access to their personal information and are able to correct, amend, or delete inaccurate information. Some exceptions exist (a) where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy, or (b) where the rights of other persons would be violated. The Access principle is a self-enforcing concept that is designed to encourage appropriate practices throughout the collection and use of personal information.

•Enforcement: Under the Enforcement principle, individuals must have the practical ability to obtain enforcement of the obligations of others with respect to the permitted or agreed-upon uses of their personal data. While there is very broad agreement as to the Enforcement principle in general, it is the specific content of the principle that, perhaps more than any other issue, causes divergence and disagreement among the various jurisdictions. Hence, the agreement and commonality with respect to this principle is as much rhetorical as it is real. Perhaps the most difficult of the specific issues under the Enforcement principle is a requirement the data subject be able to obtain, in the jurisdiction in which he habitually resides, effective enforcement of the obligations owed to him.