

END PIECE

Technology, the Internet, and Cyberspace: Challenges to National and International Privacy

By Joseph I. Rosenbaum

*In just a few hours sitting at my computer, beginning with no more than your name and address, I can find out what you do for a living, the names and ages of your spouse and children, what kind of car you drive, the value of your house and how much you pay in taxes on it. From what I learn about your job, your house, and the demographics of your neighborhood, I can make a good guess at your income. I can uncover that forgotten drug bust in college. In fact, if you are well known or your name is sufficiently unusual, I can do all this without even knowing your address.*¹

The rapid advance of information technology, and in individual and commercial use of the network of networks we call the “Internet,” has made the topic of privacy among the more significant legal issues of our time. The ease with which information can be accumulated, accessed, manipulated, used, and transmitted has not merely been the subject of intellectual legal discussion, but also the focus of critical television documentaries, newspaper articles, and heated political debate. The Internet has turned the concept of a global information-based marketplace into a reality — tied together with networks and distribution channels that make time zones and distance largely irrelevant. The merger of voice, image, data, and information processing with telecommunications networks has increased the “tradability” of information and services once confined to geographic and national barriers.

Information technologies now also permit data to be collected, compiled, analyzed, and transmitted around the world in ways never previously imagined. Information that was once difficult and expensive to collect and organize is now available with a few keystrokes. Consumers can cruise the Internet looking for information about products, services, healthcare, employment opportunities, and research subjects. This same network of networks also allows businesses to find and reach customers with significantly lower marketing costs. “The great promise of electronic commerce then is also its greatest threat. The increased market for personal information coupled with the ability to collect and compile it easily has led to an enormous increase in the amount of information collected about consumers as they perform commercial transactions and cruise the Internet.

The inherently global nature of the Internet further complicates the matter. Citizens of one country can easily visit Web sites in other countries, leaving behind valuable information.”²

Computer networks support transactions in which neither party is aware of the physical location or nationality of the other party. Must an Internet vendor comply with data protection laws in each country connected to the network or only the laws of the country in which the transaction originated or is completed? It is likely that data will be stored in multiple locations and distributed in a publicly or privately available virtual database. In a sufficiently complex computer network, it may not be apparent where the information is maintained at any point in time. National laws dependent on traditional jurisdictional laws are clearly more difficult to apply in an environment characterized by international data transfers over computer networks. A merchant engaging in a transaction who uses data in a manner that is lawful in the merchant’s country but unlawful in the consumer’s country may unwittingly discover a potentially large legal liability. Attempting to apply privacy laws on a global basis without broadly accepted, consistent international rules and procedures might be expensive, difficult, or impossible.

At the same time, as noted above, one great benefit of the Internet is its ability to make enormous amounts of information readily available and easy to manipulate, sort, and compile. Indeed, information and the ability to collect and disseminate it is the foundation of an information economy. The benefits of widely accessible and timely information and its potential for enhancing the quality of all our lives has been noted by the late Robert Maxwell in an editorial discussion published in the Spring of 1988 in Maxwell Communication’s *Global Business Magazine*. Maxwell stated: “All problems or difficulties can best be solved by the receipt of timely information packaged in a form that enables people to address them in real time. This applies at both the macro and micro levels — from governments and corporations to families and individuals — and to almost any problem you care to mention, whether it is to find a cure for AIDS, or to increase business profitability or improve an individual’s skill and, thereby, his or her earnings, or to make yourself a happier and more fulfilled person. None of these things can happen without better information.” On the other hand, it is one of the great historical ironies that both Adam Smith, the 18th century father of classical economics, and Karl Marx, one of the founding fathers of Marxist economics, considered information services and the service-based economy worthless and beneath notice. Smith stated that a service “perishes in the very instant of its production” and thus is without any value.

Information is the “capital” of an information society and can produce enormous social benefits. A global information economy depends on the free flow of information. Regardless of its perceived value, the flow of information, enabled by technology, is a pervasive and often invasive fact of today’s life, and privacy is an emotional issue, a legal issue, a sovereign issue. Whether governments or corporations own the rights to satellite photographs of their territory or businesses (or at least the right to prevent others from peering in), whether an individual “owns” information about her or his activities, whether corporations serve their customers more or less cost-effectively with access to information and who has the right to decide where the balance will lie . . . these are not

esoteric issues. In fact these are among the most hotly debated and contested issues of our time — by legal scholars, by academics, by corporations, and by governments — with profound and far-reaching implications. The challenge is to balance carefully, and in as tailored a way as possible, the competing values of protecting individuals' right to privacy against the need for the free flow of information.

Privacy is recognized as an essential human right in the Declaration of Human Rights issued by the United Nations, as well as numerous other treaties, constitutions, national laws, and judicial decisions. Privacy is implicit in such legally protected principles as freedom of assembly, freedom of association, and freedom of speech. The growth and widespread availability of technology and connectivity — the Internet, cell phones, facsimile machines, pagers, global satellite positioning systems, biometric identification tools — means that every connection, every transaction, every preference that we indicate, can be recorded, collected, traced, identified, reproduced, and transmitted. Nearly every country in the world recognizes some right of privacy — even if one argues it is merely lip service. Most countries respect the sanctity of one's home and the right to communicate with another free of eavesdropping, although only a few nations have laws or regulations which give the individual the right to control information about oneself explicitly recognized as a constitutional right (e.g., South Africa and Hungary).

Of all the rights in the international arena, privacy is also one of the most difficult to define. Not merely because privacy is as much a social and cultural value as a legal construct, but just as significantly, privacy is often a function of the context of available technology and the cultural framework in which we live — varying from nation to nation, state to state, province to province, and sometimes municipality to municipality. Consequently, our notions of privacy not only vary from country to country or cultural group, but evolve as technology evolves. It has been reported that in ancient Rome, Roman emperors traveled abroad with card registers containing data on Roman citizens,³ and Robert Ellis Smith, in his 1979 book titled *Privacy*,⁴ wrote: “Academic experts in technology and information were once shut up in a room for a day and asked to devise the most effective surveillance system imaginable for a tyrannical regime to keep tabs on its citizens. What they devised in this experiment was exactly what the bankers want to develop nationwide in the United States — a real-time electronic funds transfer system.”

Principles of privacy also have origins in other aspects of the world's history and ancestry. The Bible has numerous references to privacy,⁵ and the protection of privacy is found in early Hebrew culture, classical Greece, and ancient China.⁶ Early concepts of privacy focused mainly on the right to be alone or to be left alone (i.e., the right of solitude), while more modern principles of privacy have extended these concepts to the manner in which personal information is made available and used by others. In many countries, privacy protection defines the boundaries between one's personal life and just how far the government, commercial enterprise, other individuals, or society at large can intrude into it.

In Europe, prior to the International Telegraph Convention of 1865, territorial concepts of sovereignty over communications of citizens resulted in international messages being telegraphed to the last territorial outpost in one state, where they were transcribed and then physically carried to the adjoining state. There, the message text would be reentered and retransmitted telegraphically. Such a literal gateway approach to international information flow has a modern counterpart. Arthur D. Little, the research and consultant organization in Cambridge, produced a Decision Resources Report in 1981 that observed: "The free flow of information across international borders requires its senders and receivers either to conform to agreed upon standards or translate between standards at gateways or interfaces between systems with different internal standards."

Even the concept of a service or informational-based society is hardly a new one. In 1691 Sir William Petty, an obscure British economist, speculated that a service-based economy would be significantly more productive than one based on manufacturing. Some 250 years later, in 1941, the Australian economist Colin Clark "rediscovered" this notion. In fact, this same concept formed the basis of the popular 1973 book *The Coming of the Post-industrial Society* by noted Harvard social philosopher Daniel Bell. Bell looked forward to a golden age supported by a new type of economy dependent more on the flow of information than materials.

The recorded legal enforcement of privacy rights dates as far back as 1361, when Justices of the Peace Act in England provided for the arrest of Peeping Toms and eavesdroppers. English Parliamentarian William Pitt wrote in the 1760s: "The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow though it; the storms may enter; the rain may enter — but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement." One's home is one's castle. The right to be secure from unlawful searches and seizures and from intrusions into one's home is among the earliest expressions of the legal right to privacy. Other countries subsequently developed laws and regulations to deal with perceived abuses of privacy. Today, the concept of privacy has been woven into the fabric of the laws and regulations of most countries throughout the world. "A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organizations to intrude on that autonomy. Privacy is a key value which underpins human dignity and other key values such as freedom of association and freedom of speech. Privacy is a basic human right and the reasonable expectation of every person." (Preamble to the Australian Constitution)

At the international level, the 1948 Universal Declaration of Human Rights is probably the first multinational, international legal document which raises privacy to the level of a legally enforceable principle. The Declaration states that no one should be subjected to arbitrary interference with his privacy, family, home, or communication, nor to attacks on honor or reputation, and that each individual should have the right to legal protection against such interference or attack. In 1965 the Organization of American States proclaimed the American Declaration of the Rights and Duties of Man, which called for the protection of numerous human rights, including the right of privacy.

Most scholars attribute modern concepts of privacy in the United States to a law review article by Louis Brandeis and Samuel Warren in 1890.⁷ The impetus for their article stemmed from technological advances in photography and communications in the late 1800s, which permitted photographs to be taken without a formal “sitting.” “Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops’.”⁸ One can only imagine what Brandeis and Warren would have thought of the release by the U.S. House of Representatives, over the Internet, of recorded grand jury testimony originally given by a sitting President of the United States over secure, remote communications lines.

Beginning in the 1970s many countries began enacting legislation to protect privacy, and continuing today, privacy is one of the most hotly debated subjects in boardrooms, courtrooms, and classrooms. The interest in privacy and legal outcries to enact increasingly more comprehensive legislation and provide more effective enforcement measures is not solely a reaction to abuses or to perceived invasions of privacy. A poll published in the March 16, 1998, issue of *Business Week* noted 61% of individuals who currently do not go online or access the Internet would be more likely to begin using the Internet if they believed their personal information would be protected. Of the people who indicated they already use the Internet, 52% have never bought anything online, believing that information regarding their transactions would be used for marketing or other purposes outside their wishes and/or outside their control.

Many countries are also promulgating laws in an effort to promote electronic commerce, not merely stem abuses or invasions of privacy. Ultimately, consumers must be confident on a global basis as to how and for what purpose personal information about them may be used. In countries where consumers are increasingly uneasy with their personal information being sent around the globe, governments are including privacy within the overall framework of legislation designed to foster a consistent and uniform set of rules and regulations — or at least a common set of principles and protections — regarding electronic commerce. Countries in Eastern Europe seeking increased trade and economic benefits hope to join the European Union, and to do so, must harmonize their laws with those currently required by the EU. Thus many countries are now adopting laws based on the Council of Europe Convention and the EU data protection directive. Other countries (e.g., the United States and Canada) are reacting to privacy initiatives outside their borders by considering or enacting legislation which will ensure consistency with growing sectoral or national laws in other jurisdictions (e.g., the data protection directive of the European Union) in order to ensure that their own flow of trade is not interrupted or their own consumers or industries are not commercially disadvantaged in markets abroad.

Interest in the right of privacy increased in the 1960s and 1970s primarily due to the proliferation of computer and telecommunication technology (e.g., the first satellite, Sputnik, launched by the Soviet Union in 1957 led to growing fears of foreign espionage and surveillance). Two significant internationally recognized documents arose from these concerns. The Council of Europe’s 1981

Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data⁹ and the Organization for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.¹⁰ These two documents have had a profound effect on the adoption of laws around the world and, just as significantly, on the manner in which governments approach privacy protection around the world. Well over 20 countries have adopted the Council of Europe convention. The OECD guidelines have also been widely used in national (and even provincial or comparable local) legislation, both inside and outside OECD countries, and numerous countries which have not yet enacted comparable privacy legislation are considering doing so based on some or all of the principles codified in these documents.

Several principles of data protection have been strengthened or more detailed enforcement principles have been articulated in the EU directives (e.g., the right to know where data originated, the right to correct the inaccurate, and the right to withhold permission to use data). The European Data Protection Directive contains protections over the use of sensitive personal data relating to health or financial information. The commercial and government use of such sensitive information will require "explicit and unambiguous" consent of the individual whose information is sought to be used. The major principle in the European model is "enforceability" or, put another way, "legal accountability." Individuals must have rights that are embodied in clear and specific guidelines and rules. Individuals must be able to contact an official or authority that can investigate complaints and represent them, acting on their behalf to enforce compliance with the data protection and privacy principles embodied in the directives and the national law which implements the directives. Every EU country will have a privacy commissioner, registrar, or government-empowered agency to enforce the rules. The data protection directive requires that countries with which Europe does business and which may receive personal information about Europe's citizens and residents, will have to provide a similar or "equivalent" level of protection and a comparable means of obtaining relief against abuses or violations.

In the United States, privacy is one of the few exceptions to the principle of free flow of information. Unlike the European data directives, the hallmark of U.S. privacy law is its diversity, influenced mainly by the law's long history of development and the decentralized, federalist system of government in the United States — a system which encourages both local experimentation and state-sponsored solutions. The United States does not have a single data protection law that covers both public and private sector information, nor any one statute covering all forms of data collection by government or the private sector. Nor does the U.S. have a central commission or regulatory body that oversees privacy or data protection or to which an individual — consumer or business enterprise — may go to seek relief or enforcement.

Unlike many other countries, the United States' approach to privacy has been "sectoral," with separate laws applying to some records, generally in response to some perceived need or particular abuse, and no laws applying to many other records. There is a U.S. law protecting the privacy of video rental records,¹¹ and the stimulus for many of the privacy-related laws or regulations in the

United States is the perception that regulation of specific types of information is the only mechanism to protect privacy. Critics of this approach cite these “knee jerk” reactions to abuses as perfect examples of legislators and judges creating loopholes that others will slip through. They cite the European approach to privacy and data protection (through registrars and centralized monitoring and enforcement agencies) as the single largest contribution to the advancement of legal privacy protection theory in the last 20 years and perhaps the last century.

The U.S. approach, however, is not simply reluctance by citizens to confront privacy issues on a comprehensive basis. Rather, it is a product of differing perceptions U.S. citizens hold from their brethren in other countries concerning the role of government. Modern privacy theory may have its origins in the United States, but Americans still mistrust big government and regulation that touches individuals’ personal lives. Citizens in many other countries believe that government is responsible for protecting and helping them — further evidence that normative values and expectations of privacy (certainly those that represent legally enforceable expectations of privacy) are highly subjective and context-sensitive. Advocates of the European approach to privacy cite the “broad principles - specific interpretation” approach as a compromise between the reactive U.S. approach and those who favor self-regulation or virtually no government regulation at all. The omnibus approach adopted by European countries establishes privacy standards that are independent of technological and market considerations. By establishing broadly applicable standards, the Europeans ensure that privacy is considered in the planning stages of new technology or activities, rather than at a less efficient and less effective point in the process. The United States is rarely, if ever, able to anticipate technology with privacy laws or policies and, thus, the legal protection of privacy tends to be reactive, not proactive.¹²

Throughout the privacy debate in virtually every country in the world and certainly on an international scale, technology has been the driving force that has increased the tension among business enterprise, which cannot effectively function without the right to transfer information; individuals, concerned that information may be accumulated, used and provided to others without their knowledge or permission; and governments, who not only believe that citizens’ rights may be jeopardized if private information is transferred beyond their borders, but also worry that their national sovereignty — the capacity to independently make and influence decisions about resources and information about their nation — may be compromised.

A 1989 report on Electronic Data Interchange notes “. . . the question will increasingly arise as to which should take priority, the need for efficient, immediate economic information or the need to protect individual privacy.”¹³ The contention between the commercial need to exploit information for cost-effective, innovative benefits to the consumer and the need to ensure effective safeguards for privacy of the individual has long been a concern of government, citizens, and businesses throughout the world. Considerable debate has surrounded the question of what constitutes an adequate level of protection and by what yardstick such protections should be measured. Consider the following examples requiring this balancing process:

- Medical research often depends on individuals not knowing their behavior is being studied. While accepted research practices safeguard privacy through a variety of means (aggregation of data, agreements, internal procedures), such research would be impossible if individuals were given unrestricted access to their own medical records.
- Would the quality of human resource services deteriorate if there were restrictions on the flow of personal information in companies' information gathering during the hiring process or in providing medical insurance or other employee benefits?
- Restrictions on the free flow of information could impede the ability to verify an individual's credit card number and possibly prevent or limit a consumer from traveling or doing business freely. Customers of financial institutions could be denied access to ATMs from other networks, banks, or foreign branch offices.
- Human and civil rights activists throughout the world are critically dependent upon privacy and anonymity in order to promote their causes and disseminate information. Indeed, the basic principles of free speech and political dissent were published anonymously in the United States (The Federalist Papers) under the pseudonym "Publius."

Territorial privacy has traditionally been associated with the physical right to be left alone or undisturbed — the right to solitude noted previously. The idea that we should not be disturbed by trespassers is based on the principle that unless invited or given permission (without a "warrant"), no one is allowed to intrude into our physical space. As mentioned above, the expression "a man's home is his castle" and our legal principles of real estate and national sovereignty are examples of the application of this "spatial" notion of privacy. Territorial or spatial concepts of personal privacy manifests itself in laws relating to freedom of movement and expression, restraints against unlawful searches and seizures, and prohibitions against both physical (e.g., battery, physical injury) and non-physical assaults (e.g., discrimination, defamation, harassment, obscenity, stalking). Unlike territorial privacy, however, personal or "informational" privacy is not bounded by physical walls or geography, but by social and cultural norms — and to a large measure, technological capability.

In each case, legal principles arise and evolve to reflect society's values, and because personal privacy is highly contextual, laws evolve in each jurisdiction to mirror the perceived values of society. Privacy is legally protected and enforced, not merely because the individual has a subjective expectation of privacy, but because that expectation is considered reasonable in the context of current social practices and values. Technology, and in modern times, the Internet, changes the individual's reasonable expectation of privacy and the notion of what is socially acceptable or reasonable to expect. What is a "community," much less community standard, is increasingly difficult to define and judge in cyberspace. Previously, geographic boundaries defined neighborhoods, cities, provinces, states, and nations; today, global "chat rooms" and "Web sites" permit communities of interest to gather and share information anywhere, anytime, in any form. Consumers can just as easily shop for goods in other nations as they can around the corner.

The Internet and our growing international and global communication capabilities have highlighted another area of privacy which neither stems from physical invasions of privacy, nor direct assaults upon one's sensibilities: the disclosure, distribution, use, and abuse of information about an individual. People presume that information about themselves is their own to disclose, communicate, and control. Decisions as to what, when, and to whom disclosures are made evolve over time as relationships — personal, commercial, or governmental — change. Individuals disclose private information based on personal values and relationships (e.g., to a spouse, financial advisor, attorney, religious confessor, or physician). At other times, individuals must agree to voluntarily disclose otherwise personal facts and private information in return for other benefits. For example, one cannot obtain a home mortgage or a credit card without disclosing otherwise personal financial information to a third party. Life insurance may be contingent on the individual disclosing (or allowing a physician or healthcare professional access to) information about the state of that individual's health and some of his or her habits and lifestyle (e.g., smoking, intake of alcoholic beverages, family medical history).

Invasions of privacy occur when another person improperly obtains a fact about us or when the information is obtained by or available to a third party or the public without our permission or our knowledge. This aspect of privacy has increasingly become the focus of attention, often overshadowing physical and territorial intrusions, because of increasing technological capability and the growing pervasiveness of the Internet. The presumption of each individual's right to control information about himself or herself represents a fundamental cornerstone of our modern perception of privacy. In fact, our perception of what rights we should have and what types of information about ourselves is appropriate to disclose, when, where and to whom, continue to be evaluated and reevaluated in our information age. Significantly, a great deal of information about each of us, indeed information we may regard as quite private, is often not generated or intrinsic to the individual, but is actually created by a third party (e.g., passports, credit cards, bank accounts, and Social Security numbers). While the individual and the creator or issuer of the information have a legitimate purpose in creating and using the information, the individual obviously has a perceived interest in controlling how, when, and if the information is to be used or disclosed beyond its original purpose. Legislation, regulation, and litigation are often the results of the strong belief that there is, or should be, a continuing individual right to control such information.

Although the issues have been with us for some time, the Internet has clearly raised the level of debate. The Internet has made access to information far easier, expanding individual, commercial, and government access to numerous databases and the information they contain. A 1997 *Business Week* poll claimed that 40 million people browse the Web, almost double that of 1996.¹⁴ When every employer, medical insurer, state and local government, merchant, marketing organization, and credit card company has access to information about an individual, the potential for harm and abuse is increased substantially. The importance of quantity (rather than quality) should not be underestimated, and if the technology and availability of the Internet did nothing but increase the sheer ease and frequency of access to otherwise private information, making information available to greater numbers of people, it would represent a significant threat to privacy. However, that is

simply not the case. The Internet is increasing the sheer volume of information and individuals or entities with access, but it is also fundamentally changing the means by which we obtain and generate previously private information. If an individual wants to obtain and peruse sexually explicit material, that individual could go to a newsstand, purchase the material with cash, and read these materials only during designated personal times in the confines of that individual's designated work space, relying on the office door and desk drawer to avoid attracting the attention of an employer. Unless subject to surveillance or the object of suspicion for other reasons, these activities, not necessarily illicit or even clandestine, remain reasonably private. If that same individual uses an employer's desktop computer to access the same material through the Internet for the same purpose at the same times, technology has now given the employer (and many others) the ability to track, record, document, and use that information.

Individuals cruising the information highways are often blind to the electronic tracks they leave. Every electronic (e-mail) message, every Web site visited, every "click stream" followed and item purchased can be monitored and recorded. "Cookies"¹⁵ allow Web sites to tag visitors with unique codes that can be identified each time the visitor returns to that or any related Web site. While these cookies can be used for authentication purposes, they can also show what transactions were effected, what computer you are using and its specific Internet address, how long each visit was, and what Web "pages" were visited. Similarly, caller identification technology ("Caller ID"), originally used by telephone companies for billing purposes when transferring calls to other networks, has now become an optional feature to consumers of phone services in the United States and increasingly in other countries. The U.S. Federal Communications Commission still allows companies who are called on "800" or "900" numbers to add the caller's number to their database of customers without informing the caller.¹⁶

In each case noted above, the individual's "behavior" has not changed. Technology, however, has provided enhanced capability or changed the manner in which it is conducted, allowing it to be tracked, captured, stored, distributed and used in ways, and by entities and in nations, previously unimaginable. What one chooses to read in the reading room at the public library is not necessarily secret, but one's perception about who knows, who has access to that information, how and to what extent that information may be distributed or stored or used is quite different from our fears regarding transactionally generated information obtained by others as a result of our "surfing" the Internet. The Internet has increased the magnitude and frequency with which information can be obtained. In addition, technology has given us new means to conduct activities and new ways to capture information about these activities. Privacy is a subjective, contextual, and culturally sensitive concept. Since privacy protection arises and evolves to mirror societal values, the Internet, like the camera and telephone before it, is changing the very conceptions and expectations we have of privacy. While database marketing is hardly new, information-processing technology has increased the size, scope, and utility of databases beyond imagination. Selling access to collections of personal information is becoming more widespread, and the value of more and better information increases as demand for more and better data grows. Information has taken on signifi-

cantly greater economic value — small wonder that battles over the right to access and control information have taken on greater significance to individuals, businesses, and governments.

The Internet has also contributed to the growing “dossier effect,” whereby Internet search engines can compile huge portfolios containing extensive information about each of us from many diverse sources. With powerful search engine and information-mining technology, this represents an increasing threat as databases containing personal information become electronically cross-linked. The “dossier effect” is dangerous. When it is so easy to build a comprehensive profile of individuals, many will be tempted to take advantage of it for financial gain, vicarious entertainment, illegitimate purposes, or other unauthorized use.¹⁷ Surveys in 1988 and 1991 found errors in over 40% of all credit reports researched, and in almost 20% of those cases, the inaccuracies were such that they could lead to a denial of credit.¹⁸ Errors and inaccuracies contained in records that are linked, cross-linked, and referenced across the Internet, can be passed from database to database like a spreading virus. Can there ever be an effective way to track down and correct this information? Can a record, even an erroneous record, ever be erased? If you have ever attempted to correct information in one of the few centralized credit reporting bureau databases, imagine trying to correct information proliferating exponentially in files across the Internet. In 1995 TRW reached agreement with a Japanese credit bureau to make available Japanese credit records for Japanese citizens living in the U.S., while also allowing Japanese access to American credit records of U.S. citizens in Japan.¹⁹ Another credit reporting company with extensive international operations is Equifax, whose Canadian subsidiary is the largest provider of insurance risk management information, and operates Canada’s largest credit reporting and debt collection service. Equifax Europe operates the second largest credit network in the United Kingdom, and yet another of its subsidiaries, Transax, is the largest check-guarantee company outside the U.S.²⁰

Thus technology is not simply challenging our notions of privacy, but also our ability to deal with the very integrity and accuracy of the information increasingly available about ourselves. Technology has turned the concept of a global information-based marketplace into a reality — tied together with communications networks and distribution channels that make time zones and distance largely irrelevant. The merger of voice, image, data, and information processing with telecommunications networks have increased the “tradeability” of information and services once confined to such barriers.

From Argentina to Zambia, using digital surveillance, telephone and communications monitoring, DNA profiling, satellite surveillance, police systems, banks and credit-reporting agencies, and a whole host of computer-based information processing and communications mechanisms, information about individuals, corporations, and governments is being amassed, sorted, manipulated, transmitted, and distributed beyond our wildest imagination. Search engines on the Internet — increasingly sophisticated and powerful — present a detailed picture of people’s activities and interests. New and powerful technologies such as data mining and data matching, coupled with increasing interoperability and compatibility of systems linked together by vast arrays of networks, allow individuals, commercial enterprise, and governments access to information previously inacces-

sible and unavailable — creating the potential for invasions of privacy and rights on a scale that could scarcely have been imagined even 20 years ago.

Regardless of the views subscribed to, in whole or part or some combination of all of them, whenever one mentions the issue of privacy, everyone has a viewpoint and not necessarily a consistent one. Every government official is also an individual, every company employee is also a consumer. One's notion of privacy and what level of intrusion into information about each of us should be permitted often depends on your point of view — but which one? Indeed, even the question of what constitutes individual information versus aggregate, statistical information is another element of the debate which often yields inconsistent answers (and inconsistent feelings) from Jane Doe, the individual, versus Jane Doe, the head of marketing for a major multinational corporation, or Jane Doe, an executive of a major credit reporting agency, or Jane Doe, the Internal Revenue Service agent. Principles of privacy are not cast in concrete and will vary according to local customs and local capabilities as well as with the passage of time. The legal framework necessary to protect and enforce protected rights must also evolve to correspond to the context in which society views privacy and the technological capability available — both to abuse and protect those rights.

If politics makes strange bedfellows, the Internet has created stranger ones regarding the issue of privacy. Consider the apparent paradox of perceptions in our society which had a popular musical rock group, “The Police,” singing “every breath you take, every step you make, I’ll be watching you . . .” and yet the Director of the Federal Bureau of Investigation (FBI) in the United States has expressed his strong commitment to the protection of the individual’s right to privacy: “Without question, the use of strong cryptography is important if the Global Information Infrastructure (GII) is to fulfill its promise. Data must be protected — both in transit and in storage — if the GII is to be used for personal communications, financial transactions, medical care, the development of new intellectual property, and a virtually limitless number of other applications. Our support for robust encryption stems from a commitment to protecting privacy and commerce.”²¹

Just as the courts have dealt differently with conversations over cellular telephones than land-line-based telephone lines, courts will increasingly be called upon to interpret privacy rights in the context of technological capability. “Netiquette” is not simply a term of endearment regarding conduct on the Internet. It represents early attempts to socially define norms of conduct (and, by implication, expectations) in cyberspace.²² Virtually every reputable participant in cyberspace, from Internet service providers such as America Online and Yahoo to online companies like TheStreet.com, which provides a financial news service distributed electronically on the World Wide Web and through electronic mail (but also provides the ability for subscribers to obtain stock market quotes and track portfolios), has a code of conduct, standards of behavior, and “norms” with which they request the individual to comply as a condition for participation. While not having the force of law, these surely reflect the normative values imposed by our society. It is not beyond the realm of possibility that these codes of conduct — these rules of the road on the

information highway — will be introduced in legal proceedings as evidence of both expectations and normative values with respect to the protection of privacy.

On the one hand, there are those who would argue that changing perceptions and evolving social contexts demand that we defer and delay any legislation that attempts to deal with such a moving target. After all, such legislation could be obsolete on the day it is signed into law. But privacy legislation, database, and information protection regulation have always been difficult subjects, and many others find it equally distasteful to simply ignore the fundamental changes and permit abuses to continue while the “dust settles.” In fact, one can question whether the dust will ever really settle. If we accept the notion that many of our ideas about privacy stem from our personal experiences and perceptions, surrounded by the normative values of the society in which we live, it is likely that the law may never catch up — because the problem is not static.

As noted above, the law is deeply rooted in precedent and the past. The law looks backward in order to adjudicate the present, but the present is changing faster than ever before. The United States was an early leader in defining and defending the principles of privacy. A 1976 book by a British privacy expert asserted that America was the country with the most highly developed law of privacy.²³ The United States appears to have lost that leadership over time, and even though both federal and state governments in the U.S. have continued to enact specific privacy laws, these have, as noted above, been either sectoral or responsive to particular abuses. Global policy leadership has clearly shifted to Europe. Beginning in the 1970s many European countries enacted comprehensive data protection laws and established data protection registrars, boards, and commissions to oversee and enforce these laws.²⁴ Other countries have emulated the European model of a broad, principle-based substantive law, combined with an oversight and enforcement agency with comprehensive authority. This European model, requiring the establishment of a permanent governmental body with broad authority to interpret and enforce privacy standards, is the most significant privacy development of the past 20 years, if not the century.

On an international scale, information privacy or data protection or the control of transborder data flows appeared on the radar screen of most countries and the international community in the late 1960s and early 1970s. The benchmark international response to growing technological capability which allowed vast amounts of information to be gathered, maintained, manipulated, and distributed was a set of principles codified in the 1981 *Guidelines on the Protection of Personal Information* from the Organization for Economic Cooperation and Development (OECD). With respect to data and information these Guidelines described a number of broad principles:

- Limit the collection of data.
- Ensure the quality of data that is collected and maintained.
- Require a purpose for collecting and using the data.
- Define the permitted uses of the data.
- Establish principles for securing or safeguarding the data.

- Ensure the collection and use process is open and available to the individual whose data is collected.
- Make the gatherers, maintainers, and users of the data legally accountable.

By the end of 1996, out of the 24 OECD countries, only Australia, Canada, Greece, Japan, Turkey, and the United States had enacted these (or similar) principles into the laws that apply to organizations that process individual data. In 1995 the European Union passed a Directive on the protection of personal information, the purpose of which is to harmonize data protection legislation within the European Union and to facilitate the free flow of information. This Directive has extra-territorial implications since it requires member countries to prevent the flow of certain personal data under certain circumstances to countries that do not have a corresponding “adequate level of protection.” Over the last 20 years, numerous laws throughout the world have been enacted, agencies established, and codes adopted. The institutionalization of privacy in the world, as a legally protectable and enforceable right, continues to expand and deepen. Most privacy initiatives have taken place at the national level, although there have been international activities as well.

There are several models for privacy protection used by nations of the world and, in some cases, some segments of the international community in clusters or groups — most often, but not always, geographically based. Some countries use variations and combinations of these models. For example, the model adopted by Australia, Canada, the European Union, much of Eastern Europe, and New Zealand is that of a government agency responsible for interpreting, administering, and enforcing a comprehensive set of privacy laws and regulations. Such government agencies are responsible for administering registration and compliance requirements and, in most cases, also have the authority to conduct investigations and hearings — and even render decisions. In most jurisdictions, the agency or individual charged with this responsibility is also responsible for educating consumers and companies regarding their legal rights and responsibilities and for acting as the liaison in data protection and transborder data flow matters in the international arena. The comprehensive legislative approach to privacy generally involves broad, all encompassing “omnibus” legislation that applies to all industry sectors. Approximately 25 countries have adopted such legislation, including member states of the European Union as well as Hong Kong, New Zealand, and Taiwan. While this approach to privacy protection has been hailed as the greatest single advance in privacy over the last few decades, there is little uniformity in the powers of these agencies or individuals. Their authority and power varies greatly (and can be nonexistent for offenses committed outside their national “home” jurisdiction). More significantly, from a practical viewpoint, the resources allocated and the physical capability of these agencies or individuals to adequately enforce the laws — both affording relief to those injured and preventing abuse from occurring — is often seriously deficient.

As mentioned previously, the United States has avoided general data protection rules in favor of specific sectoral laws governing, for example, video rental records and financial privacy. In such cases, enforcement is achieved through a range of mechanisms embodied in the specific statutes or

regulations applicable to the specific privacy right involved. The difficulty with this approach is that it requires that new legislation be introduced with each new technology. As a result, protections frequently lag behind. The current lack of legal protection for genetic information in the U.S. is a striking example of the limitations of such a “responsive” or “reactive” approach to privacy. Unlike the U.S., in some countries which have adopted broad or comprehensive privacy legislation, sectoral laws are used to compliment the comprehensive legislation by providing more detailed protections and enforcement mechanisms (or even specific exemptions) for certain categories of information, such as police files or consumer credit records or military information.

Data protection can also be achieved — at least in theory — through various forms of self-regulation in which companies and industry bodies establish voluntary codes of practice. Unfortunately, the record of these efforts, especially on a global or international scale, has been disappointing. There has been little or no evidence that the aims of the codes are regularly fulfilled or that the codes themselves are uniformly and consistently followed within given industries — especially since many of the codes themselves are national rather than international in origin and scope. Adequacy and enforcement are the major problems with these approaches. Industry codes in many countries have tended to provide only weak protections and lack enforcement. This is currently the policy promoted by the governments of the United States, Singapore, and Australia. There are a variety of reasons why industry codes of conduct and privacy principles are attractive. Built on industry’s experience and expertise, they are clearly customized to each specific industry and, since they are developed by or for the industry itself, are generally less costly and burdensome to implement and enforce. In addition, at least in theory, a code of conduct adopted by a company in any given industry should apply wherever a company does business, unaffected by national borders. Again, in theory, the Internet will allow free market forces and consumer choice to produce the right balance between data protection and the free flow of information. Unfortunately, because our notions of privacy are technology, culturally, and often nationally (historically) based, and because they are evolving and dynamically changing — and not always at the same time, same pace, or for the same reasons throughout the globe — more often than not, self-regulatory theory does not translate into effective or meaningful protection.

With the recent development of commercially available technology-based systems, privacy protection has also moved into the hands of individual users. Users of the Internet can employ a range of programs and systems that will ensure varying degrees of privacy and security of communications. Technology offers solutions to many privacy concerns in the online environment, and can serve as an important tool to protect personal privacy. The Platform for Internet Content Selection (PICS), developed by the World Wide Web Consortium to filter out undesirable content, is currently being modified to offer some degree of privacy protection. The Platform for Privacy Preferences (P3P) will afford individuals the technical capability to set their individual Internet browsers according to individual privacy preferences. Once set, the technology will allow individuals to avoid Web sites or negotiate a compromise with the Web site involved. P3P will technically permit specific agreements to be reached regarding the treatment of each individual’s personal information, based on each individual’s specific preferences and tolerance for risk, based on the

perceived benefit which may be available from that particular Web site. Similar in function to P3P, Open Profiling Standard is designed to protect privacy by allowing the user alone to control the release of personal information in a secure manner. Recently, the European Commission evaluated some of the technologies and stated that the tools may have questionable long-term value and would certainly not replace the need for adequate and meaningful legal frameworks.²⁵

As an illustration of the difficulty of global information control — through combinations of technology and legislation, balancing a perceived national benefit with the risks of invasion of privacy and abuse of personal information — consider the case for nationally distributed and regulated identity (ID) cards. The type of card and its function vary greatly from country to country. While many countries have official, compulsory ID cards (e.g., Germany, France, Belgium, Greece, Luxembourg, Portugal, and Spain), many developed countries do not (e.g., the United States, Canada, New Zealand, Australia, and the United Kingdom). The threat of discrimination or political insurgency were historically the basis for many national ID systems. In more recent times, ID cards have been linked to government administration, often becoming the distribution or access vehicle for government benefits and service. On the darker side of national ID systems is the increased potential for abuse and unlawful invasions of privacy — mainly through increased capability for surveillance and detection of individual activities and transactions. In some jurisdictions, national ID cards have been challenged as constitutional impermissible invasions or intrusions on the right to privacy. For example, in 1991 the Constitutional Court in Hungary ruled that the law creating a personal identification number violated the constitutional right of privacy.²⁶

Many international data transmissions and transactions are already routine and are likely to increase unregulated by governments or national boundaries — at least so far. While there are rules regarding the international handling of regular mail, there are neither fixed routes nor fixed rules for electronic mail. An electronic message may go from Miami to Singapore through numerous countries, networks, switches, and jurisdictions, and may be stored and forwarded in or through several intermediary nations on its way to its final destination. Unlike physical mail, predicting its route or fixing the manner in which it will be handled or transmitted is often impossible, not merely impractical. The privacy protection available and afforded to such electronic mail messages is clearly subject to the laws and regulations of each jurisdiction in which it passes and in whose computer systems or switches it may be stored — whether for forwarding, temporarily or otherwise.²⁷ The United States has enacted legislation to afford a degree of legal protection to electronic messages;²⁸ however, there are clearly no equivalent levels of protection in every other country through which such messages may pass. Consequently, the uncertainty regarding the privacy protections that may be accorded electronic mail is uncertain at best.²⁹

It is noteworthy that the United States has spearheaded efforts to bolster the capability of police and intelligence authorities to “listen in” on personal communications by promoting a legal and regulatory framework that would require all digital switches and communication technology, including cell phones and satellite communications devices, to build in surveillance capability while simultaneously restricting the availability of encryption software.³⁰ Make no mistake, however.

The U.S. is not alone and government law enforcement and security agencies worldwide are seeking to establish, protect, and maintain strong capability to intercept and evaluate Internet message traffic.

Indeed, the recording of information is one of the biggest threats to privacy in our interconnected, information technology age. Every time an individual accesses a Web page, the computer (a “server”) records the Internet address (IP) along with the time and date and as much other information as may be available (e.g., duration, identity of the transmitting gateway, header information). In response to some of these perceived or real threats, “anonymous re-mailers,” “anonymizing” software, and “cookie cutter” programs have arisen to provide certain levels of technological protection to individuals — a “power to the people” approach to preventing invasions of privacy. Anonymous digital cash — frequently cited as a scheme to defraud, launder money, or avoid government control over currency and right to “mint” money — allows consumers to technologically make payments without revealing their identities.

Employees in nearly every country are also vulnerable to surveillance by their employers. The legal protections afforded to employees are generally non-existent or, at best, weak, since the employer’s rights are often “notified and agreed to” by the employee and imposed as a condition of employment. In many countries (some requiring only that the employee be given some form of notice) employers can listen and record phone conversations, read electronic mail, and not only monitor computer screens and access to communications networks, including the Internet, but even monitor actual keystrokes entered by the individual at his or her computer terminal. In the name of performance measurement, employers often can assert broad rights to analyze conversations and communications, intrude on computer files and desk files, observe activities, track personal movements using still and full motion cameras, card or other monitoring devices, conduct drug testing and demand disclosure of vast amounts of otherwise personal data. A 1991 survey of employees in the United States revealed that 62% disagreed (and of this percentage, 38% “strongly disagreed”) with employers’ use of video surveillance, even though it has been reported that two-thirds of U.S. managers spy on their workers.³¹ In the United States, there are few legal constraints on video surveillance, unlike laws in Germany and Sweden, under which employers must obtain agreement with their employees before being permitted to conduct routine surveillance.

In examining privacy legislation and protections throughout the world and in much of the foregoing discussion, it is easier to cite differences rather than the similarities. In the brief discussion that follows, some regional comparisons can be drawn by examining the laws, regulations, and court decisions of some representative countries in each region of the world.

Latin America

Numerous countries in Latin America embody strongly worded, often passionate statements regarding the individual’s legal right to privacy. Sections of Articles 18 and 19 of the Argentine Constitution state: “The home is inviolable as is personal correspondence and private papers; the

law will determine what cases and what justifications may be relevant to their search or confiscation. The private actions of men that in no way offend order nor public morals, nor prejudice a third party, are reserved only to God's judgment, and are free from judicial authority." Article 43, enacted in 1994, provides: "Every person may file an action to obtain knowledge of the data about them and its purpose, whether contained in public or private registries or databases intended to provide information; and in the case of false data or discrimination, to suppress, rectify, make confidential, or update the data. The privacy of news information sources may not be affected."³²

Article 5 of the 1988 Constitution of Brazil provides, in part: "10. the privacy, private life, honor and image of persons are inviolable, and the right to compensation for property or moral damages resulting from the violation thereof is ensured; 12. the secrecy of correspondence and of telegraphic, data and telephone communications is inviolable, except, in the latter case, by court order, in the events and in the manner established by the law for purposes of criminal investigation or criminal procedural discovery; 14. access to information is ensured to everyone and confidentiality of the source is protected whenever necessary for the professional activity."³³ Chile's Constitution secures for all persons: "Respect and protection for public and private life, the honor of a person and his family. The inviolability of the home and of all forms of private communication. The home may be invaded and private communications and documents intercepted, opened, or inspected only in cases and manners determined by law."³⁴ Similarly, the Mexican Constitution provides in part: "One's person, family, home, papers or possessions may not be molested, except by virtue of a written order by a proper authority, based on and motivated by legal proceedings. The administrative authority may make home visits only to certify compliance with sanitary and police rules; the presentation of books and papers indispensable to verify compliance with the fiscal laws may be required in compliance with the respective laws and the formalities proscribed for their inspection. Correspondence, under the protective circle of the mail, will be free from all inspection, and its violation will be punishable by law."³⁵

Despite such constitutional guarantees, in 1996 the Argentine government began a crackdown on tax evaders, reviewing credit card, insurance, and tax records of individuals. That same year, a comprehensive Argentina Passport and Federal Police Identification System was launched at the Buenos Aires airport, integrating personal data, color photos, and fingerprints.³⁶ Brazil has enacted a number of specific laws to complement the constitutional provisions. The Informatics Law of 1984 protects the confidentiality of stored, processed and disclosed data, and the privacy and security of physical, legal, public, and private entities.³⁷ Citizens are entitled to access and correct their personal information in private or public databases. The Code of Consumer Protection and Defense allows all consumers to "access any information derived from personal and consumer data stored in files, archives, registries, and databases, as well as to access their respective sources. . . . Whenever consumers find incorrect data and files concerning their person, they are entitled to require immediate correction, and the archivist shall communicate the due alterations to the incorrect information within five days. Consumer databases and registries, credit protection services, and similar institutions are considered entities of public nature."³⁸

In Chile, the Investigations Police, a civilian agency which works with the Interpol (International Criminal Police Organization) and with the military intelligence services, keeps records of all adults who are citizens, as well as all foreign residents. The Police issues identification cards that must be carried at all times.³⁹ In 1992 a surveillance center with 24-hour scanning devices was uncovered in downtown Santiago. It was run by an active army intelligence unit (DINE, incorporating former members of the secret police, the CNI) and, among other incidents, was found to have tapped into presidential candidate Sebastian Pinera's cellular phone and taped the calls of President Patricio Aylwin.⁴⁰ However, in their move to democracy since 1990, a privacy bill was introduced in 1996 covering the public and private sectors, which proposed that information can only be collected if it is authorized by law or with the express consent of the person, who must be told of its purpose.⁴¹ The bill provides that individuals have a right of access and can demand corrections or removal of information once a year. Information can only be used for the purposes for which the information was provided, and those who violate the law can be imprisoned.

In Mexico, although the Penal Code protects the disclosure of personal information held by government agencies,⁴² the General Population Act legislates and administers the National Registry of Population and Personal Identification, whose purpose is to register data and enable the reliable identification of the country's population, ultimately to issue an identity card.⁴³ While it is a member of the Organization for Economic Cooperation and Development, Mexico has not yet adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Thus, while constitutional pronouncements are typical in Latin American constitutions, implementation of actual privacy laws and enforcement of data protections for citizens is sporadic and spotty at best.

Europe

When one looks beneath the surface of European unity on privacy issues, we find a common theme, but little historical or legal consistency. The Austrian Constitution does not contain a specific right of privacy, nor is there any data-related "right of privacy" in Germany's constitution. The constitutions of Ireland or Norway do not explicitly protect the right to privacy, and the right of privacy is not explicitly protected in the French Constitution, although the tort of privacy was first recognized in France as far back as 1858.

Greece, considered by many historians to be the source of our modern governmental and societal notions of democracy, constitutionally recognizes the rights of privacy and secrecy of communications. "Each man's home is inviolable. A person's personal and family life is inviolable," and "The privacy of correspondence and any other form of communication is absolutely inviolable. The law shall determine the guarantees under which the judicial authority is released from the obligation to observe the above-mentioned right, for reasons of national security or for the investigation of particularly serious crimes."⁴⁴ The Italian Constitution has several similar provisions relating to privacy⁴⁵ and Article 22 of the Belgian Constitution, added in 1994, recognizes the right of privacy and private communications.⁴⁶ The Dutch Constitution grants citizens an explicit right to

privacy,⁴⁷ and the Portuguese Constitution has extensive provisions on protecting privacy, secrecy of communications, and data protection.⁴⁸ The Danish Constitution contains privacy and data protection provisions.”⁴⁹

Some sections of data protection law contain provisions comparable to constitutional protections and provide the right of secrecy of personal data and respect for private and family life. Numerous countries have privacy and data protection laws applicable to the protection, disclosure, and transmission of data and personal information. Constitution protections or not, European countries routinely have enacted freedom of information laws that oblige authorities to answer questions regarding their areas of responsibility, limits on the extent and nature of surveillance on their citizenry, and severe restrictions on the disclosure of sensitive information. One can argue whether some or all of these laws are more honored in their breach by law enforcement and governmental agencies; nevertheless, the laws are on the books.

Thus, despite the different historical origins and how and where the protections appear, of all the regions of the world Europe has made the greatest strides in unifying its approach to privacy legislation and enforcement and implementing a consistent framework of legal and regulatory principles in the area of data protection and personal privacy. Without an exhaustive or complete list, but to illustrate the diversity of national and cultural origin, yet highlight to growing community of purpose and approach, Austria, Spain, Denmark, Belgium, France, The Netherlands, Germany, Portugal, Greece, Norway, Finland, Slovenia, Ireland, Italy, Sweden, Switzerland, and the UK are all members of the Council of Europe and have all signed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.⁵⁰ All are members of the Council of Europe and of the Organization for Economic Cooperation and Development and, with the exception of Slovenia, have all adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.⁵¹

Eastern Europe and Russia

The Bulgarian Constitution recognizes rights of privacy, secrecy of communications, and access to information,⁵² as does the Constitution of Poland.⁵³ Similarly, the Constitution of the Russian Federation recognizes rights of privacy, data protection, and secrecy of communications.⁵⁴ While constitutional protections are common in this region of the world, abuses based on historical cultural, national, and governmental mistrust abound. Shifting national boundaries and political instability have contributed to there being widespread recognition of the need to cure the ills of past regimes, with little trust and political unity to effectuate a “privacy” agenda. Clearly, a desire to enter global markets and stimulate economic growth and reform create significant incentives for countries in this region of the world to conform their policies and legislative frameworks. In some cases, the desire to participate in markets leads to scrutiny of progress being made in this area, and as an example, in 1997 the European Commission, citing Bulgaria, stated that “considerable efforts are still needed to adopt and implement measures to meet community requirements on data protection.”⁵⁵

Legislative efforts in countries such as Estonia and Poland typify the flurry of recent activity in the area of privacy and privacy-related legislation. In June 1996 Estonia's Parliament enacted the Personal Data Protection Act, and in April 1997 it passed the Databases Act, establishing a national database.⁵⁶ Both Acts are administered and supervised by the Data Protection Department of the Ministry of Internal Affairs. The Legal Committee of Parliament exercises supervision over the Data Protection Supervision Authority. The Data Protection Department is currently developing legislation that would make it independent and bring the law in line with the EU Directive.⁵⁷ Unfortunately there are often relatively few individuals to actually carry out the functions required.⁵⁸

Australia and New Zealand

The Australian Constitution contains no express provisions relating to privacy. The principal Australian federal statute concerning the protection of personal data is the Privacy Act of 1988, which created a set of information privacy principles applicable to most federal government agencies and which are based on the OECD Guidelines.⁵⁹ Additional rules that relate to consumer credit information were added to the law in 1989 and are applicable to both the private and public sector.

As with legislation in the European Union, Australia has an Office of Privacy Commissioner responsible for handling complaints, auditing compliance, community awareness and education, and acting in an advisory capacity to the government in internal and international matters.⁶⁰ Although Australia has had a statute which applies to the government's use of personal information since 1988, after considering whether to enact additional privacy legislation applicable to the private sector's use of personal information, the Australian government decided to promote self-regulation. In February 1998 the Australian Government issued *The National Principles for the Fair Handling of Personal Information*. These principles are intended to be guidelines for voluntary privacy codes of conduct developed by industry and are based on the OECD Guidelines.

The persistence of "record linkage" or "computer matching" in New Zealand has been the primary motivating force for the passage of the New Zealand Privacy Act in 1993, one of the only comprehensive data protection laws outside Europe that includes both public and private sectors.⁶¹ The Act has been amended twice since its enactment and applies to any information about an identifiable individual, whether the information is processed automatically or manually.⁶² Similar to the Australian Privacy Act, the New Zealand Privacy Act creates information privacy principles based on the 1980 OECD guidelines. In addition, the Act also contains principles relating to information matching programs run by government agencies.

New Zealand has a privacy commissioner that oversees compliance with the Act, but the commissioner does not function as a registration or notification authority.⁶³ The privacy commissioner's main role is promoting awareness, monitoring legislation and government policies, handling complaints, approving codes of practice, approving exemptions from the privacy principles, and reviewing information matching programs for compliance with the Act.

New Zealand is a member of the Organization for Economic Cooperation and Development and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. New Zealand is also one of six countries involved in a study by the European Commission in connection with the evaluation of laws of “third countries” and the parameters regarding a determination of whether such laws provide “equivalent protection” meeting the European Union’s data protection requirements.

Asia

Japan and South Korea are members of the Organization for Economic Cooperation and Development and have adopted the OECD Guidelines on Privacy and Transborder Dataflows of Personal Data. While privacy principles are embodied in several articles of the Japanese Constitution⁶⁴ and included directly in the Constitution of South Korea,⁶⁵ the Singapore Constitution, which is based on the British system, contains no explicit right to privacy, nor does Singapore have any comprehensive data protection or privacy law.⁶⁶

The principal legislative pronouncement on privacy in Japan is the Act for the Protection of Computer Processed Personal Data Held by Administrative Organs passed in 1988, which governs the use of personal information in computerized files held by government agencies.⁶⁷ Based on the OECD guidelines, it requires governmental agencies to limit the collection of personal data to relevant information and to publicly list their files. The Act also provides that the information collected for one purpose cannot be used for “other than the file holding purpose.” While there was relatively little activity on the privacy front for many years, more recently there has been a spate of privacy-related initiatives, legislation, and proposed legislation, ostensibly to promote greater trade and electronic commerce with Japan’s global trading partners.

In 1997 the Ministry of International Trade and Industry (MITI) issued Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector. In 1998 the Ministry established a new system for the granting of “privacy marks” to businesses committing to the handling of the personal data in accordance with the MITI guidelines — something akin to a “seal of approval.” Companies that fail to comply with industry guidelines are excluded from industry bodies.⁶⁸ In June 1998, then-Prime Minister Hashimoto announced that an agreement had been reached with the United States for self-regulation for privacy measures on the Internet except for certain sensitive data.⁶⁹ In June 1998, Japan’s Ministry of Posts and Telecommunications established a study group to examine privacy in telecommunications services, and in July of that same year the government recommended that a new law to protect credit reports be enacted.⁷⁰

In Korea, the Act on the Protection of Personal Information Managed by Public Agencies of 1994 sets rules for the management of computer-based personal information held by government agencies and is based on the OECD privacy guidelines. Under the Act, government agencies must limit data collected, ensure their accuracy, keep a public register of files, ensure the security of the information, and limit its use to the purposes for which it was collected. The Act is enforced by the

Minister of Government Administration. Credit reports are protected by the Act Relating to Use and Protection of Credit Information of 1995.⁷¹ The Ministry of Commerce, Industry and Energy proposed a set of guidelines for electronic commerce legislation in May 1998 (i.e., “Basic Law for Electronic Commerce”), including protecting privacy in the digital trade environment.⁷²

All Internet service providers in Singapore are controlled by government-owned or government-controlled companies, and anyone wishing to obtain an Internet account in Singapore must provide their national ID to obtain an account.⁷³ ISPs reportedly provide information on users to government officials without legal requirements on a regular basis. In 1994 an Internet provider serving the academic and technical community scanned e-mail of members looking at large file sizes typical of pornographic material. In September 1996, in the first instance of enforcement of Singapore’s Internet regulations, a man was fined for downloading sex films. Afterwards, citizens were assured by the Singapore Broadcasting Authority (the regulatory agency for electronic media under the Ministry of Information and the Arts) that they do not monitor e-mail messages or what sites people access or visit.⁷⁴

Singapore’s National Internet Advisory Board has proposed an industry self-regulatory “E Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce.”⁷⁵ The code, proposed in September 1998, would require confidentiality of business records and personal information and prohibits interception of communication, absent legal process.

Canada

There is no explicit right to privacy in Canada’s Constitution and Charter of Rights and Freedoms. Since 1983 the Access to Information Act⁷⁶ and the Privacy Act⁷⁷ provide individuals with access to personal information held by the federal public sector. The Privacy Act contains provisions that govern the collection, correction, confidentiality, and use of personal information. Individuals may request written, video, and computer records directly from the institution with the information. The Privacy Act and the Access to Information Act are overseen by independent commissioners⁷⁸ with the power to investigate and make recommendations, but with no ability to adjudicate disputes or complaints nor issue binding decisions. The vast majority of personal information collected by the private sector is on the provincial level and is generally not protected by provincial law, although Quebec may be the only jurisdiction in North America with a comprehensive law protecting both private and public sector information. On the federal level, the Telecommunications Act⁷⁹ protects the privacy of individuals and the Bank Act⁸⁰ and Insurance Companies Act⁸¹ provide for rules governing the use of customer information.

Republic of India

The Constitution of 1950 does not expressly recognize the right to privacy⁸² nor does India have any comprehensive or general privacy law. In July 1998 a National Task Force on IT and Software

Development, set up by the Prime Minister's Office, submitted an "IT Action Plan" calling for the creation of a "National Policy on Information Security, Privacy and Data Protection Act for handling of computerized data." Using the Data Protection Act in effect in the United Kingdom, the Task Force recommended the enactment of a number of laws, including privacy and encryption relating to digital commerce and cyberspace.⁸³

South Africa

Presumptively responding to abuses during the time when South African's apartheid policies were in effect, the South African Constitution states, "Everyone has the right to privacy, which includes the right not to have (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed," and "(1) Everyone has the right of access to (a) any information held by the state, and; (b) any information that is held by another person and that is required for the exercise or protection of any rights."⁸⁴ Privacy in South Africa is also protected under the broad principles of common law (i.e., so called "*actio injuriarum*," which deals with infringement of personality rights, including the right to privacy). South Africa introduced the Open Democracy Bill in July of 1998, which is a comprehensive privacy and freedom of information law covering the public and private sector;⁸⁵ however, despite Constitutional provisions and common law principles, South Africa currently does not have a privacy commission, nor is there any specific statutory privacy protection in South Africa.

Although not universal by any means, in many countries other than the United States the most common approach to privacy legislation and regulation currently being implemented at the national level is through the passage of laws which broadly define privacy principles applicable to government and private sector records.⁸⁶ That being said, information technology is advancing so rapidly that privacy controls may, as a practical matter, become harder to draft and enforce on a national level. The ability to enforce laws and even national policy regarding privacy is decreasing exponentially as time, distance, and national boundaries become increasingly irrelevant to communications, information disclosures, and economic transactions.

As may become increasingly clear, international uniformity of regulation is likely to depend in large measure on the extent to which activities routinely involve the transfer of personal information across national borders. Since information and technology, most notably the Internet, are increasingly important in international and corresponding national commerce, the pressures for uniformity on an international scale are likely to increase and may well be the major privacy issue as well as the impetus for privacy legislation and regulation in the 21st century.

For example, since they were developed virtually simultaneously by individuals and organizations working together, striking similarity exists between the OECD Guidelines and the Council of Europe Convention. While there is no formal code of fair information practices per se, both documents contain broad general principles of fair information practices based on the following eight principles:

- Openness — the existence of record-keeping systems and databases be publicly known, along with a description of purpose and use of data.
- Individual Participation — individuals have a right to see, correct, and, if necessary, remove their individual data to ensure it is timely, accurate, relevant, and complete.
- Collection Limitation — data should be collected by lawful and fair means, and where appropriate, with knowledge or consent.
- Data Quality — data should be accurate, complete, timely, and relevant to the purposes for which it is used.
- Use Limitation — limits internal uses to those specified at the time of collection.
- Disclosure Limitation — restricts the external communication of data without consent or other legal authority.
- Security — requires data to be protected by reasonable safeguards against such loss, unauthorized access, destruction, use, modification, or disclosure.
- Accountability — requires record keepers to be accountable for complying with fair information practices.

By way of comparison, and despite the oft cited differences in U.S. law from the European models, in 1997 the Clinton Administration in the United States released its policy paper titled “A Framework for Global Electronic Commerce,” borrowing heavily from the European models of fair information practices. This at the same time it reaffirms the U.S. government’s official commitment to effective self-regulatory privacy protection. In January 1998, subsequent to the release of the U.S. policy paper, the U.S. Department of Commerce released a draft of a discussion paper describing some familiar elements the administration in the U.S. considers necessary for such self-regulation:

- Awareness — Consumers need to know the identity of the collector, the intended uses, and the means they may use to limit disclosure. Companies can do so through privacy policies, notification, and/or consumer education.
- Choice — Consumers must have a choice (and the means to exercise such choice) as to whether and how their information is used. For certain kinds of information, companies should not use personal information unless its use is explicitly consented to by the individual or, in the case of children, a parent or guardian.
- Data Security — Reasonable measures must be in place to assure reliability for its intended use and reasonable precautions to protect it from loss, misuse, alteration, or destruction should exist.
- Access — Consumers should have access to information and be able to correct or amend it as necessary.
- Recourse — Consumers must be provided readily available and affordable mechanisms by which complaints can be resolved.
- Verification — Companies must certify that claims about their privacy practices are true and that these practices have been implemented.
- Consequences — Failure to comply with these fair information practices should have consequences.

It remains important to bear in mind, however, that despite broad similarities in approach and the conceptual policy issues discussed, the OECD Guidelines, Convention of Europe, and the U.S. government's policy papers have significant differences. For example, the Convention applies only to automated processing of personal information, while the OECD Guidelines are not limited to automated data and include manual files and processing. The Convention is legally binding for countries that have ratified it, while neither the OECD Guidelines nor the U.S. policies are legally enforceable. None of these schemes offer any specific details or standards regarding actual privacy protection methodologies or information handling, nor do they contain any specific guidelines regarding enforcement. The OECD and Convention focus on the role of government in establishing whatever standards and enforcement mechanisms are to exist, while the U.S. approach remains "reactive," encouraging private rights of action for failures of companies to live up to their advertised codes — assuming they choose to adopt and announce them — with only a suggestion as to the possibility of regulatory action (e.g., Federal Trade Commission) for failure to follow up. The OECD Guidelines require data controllers to be accountable for both registration and administration, as well as compliance, while the Convention of Europe requires only that the signatories establish appropriate sanctions and remedies for violations of data protection laws.⁸⁷

Stalling efforts toward global uniformity is the broad diversity in existing and emerging legal frameworks, differing cultural and societal perceptions of privacy and its implications, the wide disparity in technological capabilities in the world community, some who favor no regulation, many who favor voluntary regulation and those who favor regulation designed to protect their own national interest, at the expense of less structured or weaker regulation at the international level. In addition, the continuing tension between individuals, commercial enterprise, and government — and even within differing segments of each of these constituencies — makes common approaches and common solutions among the greatest challenges of the coming millenium.

In 1984 the polling organization, Gallup, conducted a survey to assess the extent to which individuals in six countries perceived that George Orwell's vision of Big Brother in his classic *1984* had become less fiction and more reality. Individuals were asked to respond to the statement that "there is no real privacy because the government can learn anything it wants about you." Individuals agreed with that statement in the following percentages recorded by the survey: United States (47%); Canada (68%); Britain (59%); West Germany (18%); Switzerland (18%); and Brazil (43%). Between 60% and 70% of individuals surveyed in the U.S., Canada, and Australia believe they have lost control over personal information, and it is clear this fear is attributable to the spread of information technology. Between 70% and 80% of Americans, Canadians, and Australians believe that current uses of computers are threatening or eroding personal privacy.⁸⁸

Deciding what privacy rules, laws, or standards apply to information, individuals, and commercial enterprise in an international environment is difficult enough. Enforcement of these standards poses even more difficult challenges across national boundaries. Individuals can bring lawsuits to enforce their rights, but the former General Counsel to the Privacy Protection Study Commission in the United States testified that the Privacy Act was "to a large extent . . . unenforceable by . . .

individual[s],” primarily because it is difficult to recover damages and no injunctive relief is available.⁸⁹ In fact, enforcement of privacy rights is often impossible for foreigners as a matter of law, since most privacy laws apply only to citizens or residents. Bringing and conducting a lawsuit in a foreign country is difficult enough, and the problem is magnified by a lack of uniform rules or consistent privacy regulations. While data protection authorities in “EU” countries may investigate complaints from individuals, it is difficult for any individual to pursue a remedy within his or her “home” country. Imagine the obstacles one faces attempting to pursue relief overcoming language, cultural, legal, currency, and geographic obstacles. These are formidable barriers for even the most skilled individuals and, quite frankly, are not realistic for most.

Conclusion

From the foregoing discussion, it should be clear that conflicting privacy laws and rules among a wide variety of nations, and even aggregations of nations, will continue (at least for the foreseeable future) to present unavoidable political, cultural, legal, and regulatory policy problems. Agreement on general policy principles has not and probably will not be sufficient to establish the common procedures needed to implement a uniform or consistent set of privacy rules on an international basis. Implementation and enforcement of any policy, law, or regulation require additional rules by which actual behavior is measured and governed, recognizing that differences are inevitable. It has been noted (and it is worth repeating) that diversity is not always a bad thing. Understanding differences and using a “best practices” approach to unifying procedural and substantive privacy rules among nations can serve as a valuable source of both experience and expertise. Although differences may often mean that specific remedies will be difficult or even unavailable, one needs to appreciate and understand that these rules often must vary to reflect local priorities, cultures, industries, and needs. It cannot be avoided that differences will produce conflicts across borders.⁹⁰

It should also be clear that some governments, for good or bad reasons, will continue to resist harmony or avoid adhering to privacy principles that are perceived to be at odds with the ability to favor national industries or interests, or to simply maintain control. While the similarities between the U.S. policy, OECD and Council of Europe positions is laudable, and despite the substantial commitment of the European Union harmonized approaches to difficult and complicated matters such as privacy, it literally has taken years to achieve the current generalized agreement on the protection of personal information. It is unfortunately increasingly obvious that the United States itself represents a major obstacle to uniform, government-sponsored, global privacy initiatives. The U.S. business community is likely to continue to oppose conformance to any international set of required principles unless and until the failure to join results in some serious real or perceived economic or commercial disadvantage, notwithstanding the fact that there may be some companies and industries which will continue to need to conduct business and operate within the framework of some foreign privacy legislation and regulation. Indeed, some scholars believe that existing national laws actually represent a significant obstacle to uniform regulation. If, the primary interest of any country is not to achieve consistency but to preserve their unique national rules,

then consistency will only be achieved if harmony incorporates (and, to some extent, only replicates) that nation's specific rules.

As has been repeated many times and in many different ways, information and communications technology has already torn asunder jurisdictional boundaries which previously contained individuals, corporations, and information, not to mention government regulation. The OECD Guidelines and the Council of Europe Convention were adopted almost two decades ago, well before the Internet was a growing commercial or household word. Even the European Union's broad and comprehensive conceptual approach to privacy which has been hailed as independent of specific technology could not (and does not) anticipate much of the change that technology has wrought. In fact, in a paperless, digital, information-based world, many of the legal assumptions upon which traditional protections and regulations have relied for centuries are beginning to crumble. The technological and informational revolution has been overwhelming to say the least.

Obviously, if governments cannot deal with unifying international privacy effectively, there are alternatives.⁹¹ The private sector may develop voluntary privacy codes without the participation of governments.⁹² Significantly, since Internet and digitally wise individuals tend to be more concerned about privacy, it may become a marketing advantage for commercial enterprise to adopt or agree to industry or government-sponsored privacy codes and highlight its voluntary compliance to distinguish it from competitors. Even if private industry, government-sponsored initiatives, and general principles can be somehow blended and combined to present an acceptable set of principles that nations can adopt in principle, absent effective enforcement, these principles will be simply be that — a set of principles without any real practical meaning or effectiveness to the constituency the principles are intended to protect. Some proponents of self-regulation argue that if international and multinational industry leaders, working with consumers and other individual interest groups, developed and implemented voluntary privacy codes, governments might be encouraged or pressured to conform their laws to them.⁹³

In conclusion, privacy was a legally protected right, an important cultural and societal value, the underpinning of our modern concepts of respect and dignity for the sanctity of one's person, one's domicile and one's private activities, hundreds of years before the invention of information processing systems, communications technology, and the Internet. That being said, modern technology has moved privacy issues from the local to the national and now to the international sphere primarily because digital information processing and communications capability is not merely a technological advance. There are fundamental changes taking place in the way we work and do business, the way we educate and entertain ourselves, the way we communicate and interact with our world — indeed the way we experience our environment — truly in an increasingly global sense. One can only wonder if a shipbuilder from Gdansk, Poland, would have been able to gather the support and affect the fate of the world if the information and message had not been available to large segments of both the national and international community through broadcast and informational vehicles unknown a mere decade earlier. It is one of the great ironies of history that large numbers of academics, scholars, and great thinkers accurately predicted that man would someday

walk on the moon. Indeed, many even surmised the clothes or outerwear and the vehicles necessary to successfully accomplish such an endeavor. What no one predicted or could have imagined is that the entire world would be able to watch the event on publicly available television. We cannot predict whether the global community, spurred by the proliferation of information and technology, will be pressured to unify privacy principles and apply commonly accepted procedures to allow individuals throughout the world to benefit from consistently and widely accepted protections. But we can try. A famous philosopher once said, "We must welcome the future, remembering that soon it will be the past; and we must respect the past, remembering that once it was all that was humanly possible."⁹⁴

Joseph I. Rosenbaum is head of the Electronic Commerce group in the New York office of Greenberg Traurig, a U.S.-based full-service international law firm. Mr. Rosenbaum chairs the Information Technology & Global Networks Committee of the American Bar Association's Section of Science and Technology, is a past council member of the Section, and is also an ABA member of the National Conference of Lawyers and Scientists. Mr. Rosenbaum writes and lectures extensively both domestically and internationally, and is an Adjunct Professor of Law at New York Law School, where he teaches The Law of Electronic Commerce and Information Technology.

¹ Lane, Carole A., Naked in Cyberspace: Online Magazine's Guide to What You Can Find Out Online About Anyone (Burwell, Helen and Davies, Owen B., Eds., 1st Edition 1997).

² Privacy And Electronic Commerce, Draft Prepared by United States Department of Commerce, June 1998.

³ Hamelink, C., Transnational Data Flows in the Information Age, 9 (1984).

⁴ Smith, *Privacy*, Anchor/Doubleday, 1979.

⁵ See Barrington Moore, *Privacy: Studies in Social and Cultural History* (1984).

⁶ *Ibid.*

⁷ Brandeis, Louis D. & Warren, Samuel D., *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

⁸ Brandeis, *supra* note 1, at 195.

⁹ Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Strasbourg, 1981.

¹⁰ OECD, Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data, Paris, 1981.

¹¹ Video Privacy Protection Act of 1988, Pub. L. No. 100-618, § 102 Stat. 3195 (1988) (codified as amended at 18 U.S.C. § 2710 (1994)).

¹² Gellman, Robert M., *Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules*, 41 Vill. L. Rev. 129, 146-147 (1996).

¹³ Stanbrook & Hooper, "Data Protection Legislation and their Impact on EDI," TEDIS Legal Workshop, Brussels, June 19-20, 1989.

¹⁴ *Internet Demographics* (Apr. 25, 1997) <http://www.healinghearts.com/directory/web-demographics.html>.

¹⁵ "Cookies" or Persistent Client-Side Hyper-Text Transfer Protocol ("HTTP") are files containing computer code written onto the user's computer hard drive when a web site is visited.

¹⁶ Scott, Gini G., *Mind Your Own Business: The Battle for Personal Privacy*, 346 (1995).

¹⁷ Ian Goldberg et al., *Privacy-Enhancing Technologies for the Internet* (last modified Jan. 21, 1997) <http://www.cs.berkeley.edu/~daw/privacy-compcon97-www/privacy-html.html>.

¹⁸ DeCew, Judith Wagner, In Pursuit of Privacy: Law, Ethics & the Rise of Technology (Cornell University, at pg. 50 (1997).

¹⁹ TRW Communications Department, TRW And Japanese Credit Bureau To Open Way For Lender Access Of "Homeland" Consumer Credit Data (Press Release, June 19, 1995).

²⁰ This information was retrieved from Equifax, Inc. at <http://www.equifax.com>. See also, "Equifax Broadens European Market, Signs Joint Venture For Credit Reporting In Portugal" (Press Release, July 20, 1995).

²¹ Impact of Encryption on Law Enforcement and Public Safety: Hearing Before the Sen. Comm. on Commerce, Science, and Transportation, 104th Cong. 5 (1996) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation).

²² The term "cyberspace" was originally coined by William Gibson in his 1984 book, *Neuromancer*, and actually it referred more to what we currently think of as virtual reality, rather than to the Internet and the World Wide Web.

²³ Paul Sieghart, Privacy And Computers 11 (1976).

²⁴ Sweden Data Act of 1973 established a Swedish Data Inspection Board; France passed the Law on Informatics, Data Banks and Freedoms in 1978, which established a National Commission on Informatics and Freedoms.

²⁵ Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS).

²⁶ Constitutional Court Decision No. 15-AB of 13 April 1991.

²⁷ Messages could be captured and stored in intermediate countries. See Charles R. Babcock & Don Oberdorfer, *Computer Detective Found Crucial Data; Intern's High-Tech Sleuthing Led to Files*, Wash. Post, Feb. 28, 1987, at A10; see also House Comm. On Government Operations, Taking A Byte Out Of History: The Archival Preservation Of Federal Computer Records, H.R. Rep. No. 978, 101st Cong., 2d Sess. 9-10 (1990).

²⁸ Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848-73 (1986) (codified as amended at 18 U.S.C. § 2510 (1994)).

²⁹ The risks of legal interception of electronic mail must be distinguished from the unauthorized or illegal interception. There are techniques, such as encryption, that minimize the consequences of interception. Government regulation of encryption is a highly controversial constitutional, policy and political issue. See, e.g., A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, The Clipper Chip, and the Constitution*, 143 U. Pa. L. Rev. 709, 712 (1995); See Also Dorothy E. Denning & William E. Baugh, Jr., *Key Escrow Encryption Policies And Technologies*, 41 Vill. L. Rev. 289 (1996).

³⁰ See Banisar and Davies, *The Code War*, Index on Censorship, January 1998.

³¹ American Management Association, Report on Electronic Monitoring & Surveillance, 1997. <http://www.amanet.org/survey/elec97.htm>.

³² Constitucion de la Nacion Argentina (1994).

³³ The Constitution of Brazil, 1988.

³⁴ Constitution of Chile, 1980, Article 19.

³⁵ Constitucion Politica de los Estados Unidos Mexicanos, Article 16.

³⁶ Business Wire, Sept. 12, 1996.

³⁷ Law No. 7.232, October 29, 1984.

³⁸ Law No. 8078, September 11, 1990.

³⁹ Chile: A Country Report, 1994: U.S. Library of Congress, http://lcweb2.loc.gov/cgi-bin/query/D?cstdy:26:./temp/~frd_IHzm:

⁴⁰ Television Nacional de Chile, BBC Summary of World Broadcasts, September 26, 1992. Latin America Weekly Report, October 8, 1992.

⁴¹ Protection of Personal Data, House of Deputies, November 1996.

⁴² Código Penal Federal, Article 214.

⁴³ <http://www.hri.ca/fortherecord1997/documentation/commission/e-cn4-1997-67.htm>.

⁴⁴ Constitution of Greece, Adopted: 11 June 1975.

⁴⁵ Constitution of the Republic of Italy, Adopted 22 Dec 1947.

⁴⁶ Constitution of Belgium which states "(1) Everyone has the right to the respect of his private and family life, except in the cases and conditions determined by law. (2) The laws, decrees, and rulings alluded to in Article 134 guarantee the protection of this right."

⁴⁷ Constitution of the Kingdom of the Netherlands 1987. Article 10: "(1) Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament. (2) Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data. (3) Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament." Article 13: "(1) The privacy of correspondence shall not be violated except, in the cases laid down by Act of Parliament, by order of the courts. (2) The privacy of the telephone and telegraph shall not be violated except, in the cases laid down by Act of Parliament, by or with the authorization of those designated for the purpose by Act of Parliament."

⁴⁸ Constitution of the Portuguese Republic, 2 April 1976, Article 26: "(1) Everyone's right to his or her personal identity, civil capacity, citizenship, good name and reputation, image, the right to speak out, and the right to the protection of the intimacy of his or her private and family life is recognized. (2) The law establishes effective safeguards against the abusive use, or any use that is contrary to human dignity, of information concerning persons and families. (3) A person may be deprived of citizenship or subjected to restrictions on his or her civil capacity only in cases and under conditions laid down by law, and never on political grounds." Article 35: "(1) Without prejudice to the provisions of the law on State secrecy and justice secrecy, all citizens have the right of access to the data contained in automated data records and files concerning them as well as the right to be informed of the use for which they are intended; they are entitled to request that the contents thereof be corrected and brought up to date. (2) Access to personal data records or files are forbidden for purposes of getting information relating to third parties as well as for the interconnection of these files, save in exceptional cases as provided for in the law; and Article 18: (3) Data processing may not be used in regard to information concerning a person's philosophical or political convictions, party or trade union affiliations, religious beliefs, or private life, except in the case of non-identifiable data for statistical purposes. (4) The law defines the concept of personal data for the purposes of data storage as well as the conditions for establishing data banks and data basis by public or private entities and the conditions of utilization and access. (5) Citizens may not be issued all-purpose national identification numbers. (6) The law defines the provisions applicable to transborder data flows establishing adequate norms of protection of personal data and of any other data in which the national interest is justified." Article 35 was amended in October 1997.

⁴⁹ <http://www.uni-wuerzburg.de/law/da00t.html>.

⁵⁰ Signed 28/01/81. Ratified 30/03/88. Entered into force 01/07/88.

⁵¹ Switzerland is not a EU member state but has been granted associate status. Although Norway is not a member of the EU, it is a party to the 1992 Agreement on the European Economic Area (EEA). As such, Norway is required to comply with the EU Directive before it is formally incorporated into the EEA.

⁵² Constitution of the Republic of Bulgaria of 13 July 1991.

⁵³ The Constitutional Act of 1997, Articles 47 and 51.

⁵⁴ Constitution of the Russian Federation, 1993, Article 23, 24 and 25 which provide: "1. Everyone shall have the right to privacy, to personal and family secrets, and to protection of one's honor and good name. 2. Everyone shall have the right to privacy of correspondence, telephone communications, mail, cables and other communications. Any restriction of this right shall be allowed only under an order of a court of law."

“1. It shall be forbidden to gather, store, use and disseminate information on the private life of any person without his/her consent. 2. The bodies of state authority and the bodies of local self-government and the officials thereof shall provide to each citizen access to any documents and materials directly affecting his/her rights and liberties unless otherwise stipulated under the law.” “The home shall be inviolable. No one shall have the right to enter the home against the will of persons residing in it except in cases stipulated by the federal law or under an order of a court of law.”

⁵⁵ <http://europa.eu.int/comm/dg1a/agenda2000/en/opinions/bulgaria/b1.htm>.

⁵⁶ Kaidi Oone, “Estonian IT Legislation,” Baltic IT&T ‘98 Conference Proceedings, Riga, Latvia, April 15-18, 1998.

⁵⁷ <http://www.sisemin.gov.ee/ako/eng/about.html>.

⁵⁸ <http://www.sisemin.gov.ee/ako/>.

⁵⁹ Privacy Act 1988 (Cwth) http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/longtitle.html.

⁶⁰ <http://www.privacy.gov.au/>.

⁶¹ The Privacy Act 1993, <http://www.knowledge-basket.co.nz/privacy/legislation/1993028/toc.html>.

⁶² The Privacy Amendment Act 1993 <http://www.knowledge-basket.co.nz/privacy/legislation/1993059/toc.html>, The Privacy Amendment Act 1994 <http://www.knowledge-basket.co.nz/privacy/legislation/1994070/toc.html>.

⁶³ <http://www.knowledge-basket.co.nz/privacy/top.html>.

⁶⁴ Constitution of Japan, November 3, 1946, Articles 21 and 35: “Freedom of assembly and association as well as speech, press and all other forms of expression are guaranteed. No censorship shall be maintained, nor shall the secrecy of any means of communication be violated.”

⁶⁵ Constitution of the Republic of Korea, 17 July 1948. Article 17 provides: “The privacy of no citizen may be infringed.”

⁶⁶ Constitution of the Republic of Singapore, 16 September 1963.

⁶⁷ The Act for the Protection of Computer Processed Personal Data held by Administrative Organs, Act No. 95, 16 December 1988 (Kampoo, 16 December 1988).

⁶⁸ Ministry of International Trade and Industry (MITI) ‘Japan’s views on the protection of personal data’ (April 1998).

⁶⁹ US Japan Joint Statement on Electronic Commerce, May 15, 1998. <http://www.ecommerce.gov/usjapan.htm>.

⁷⁰ Jiji Press Ticker Service, June 12, 1998.

⁷¹ Act Relating to Use and Protection of Credit Information, Law No. 4866, Jan. 5, 1995.

⁷² Nikkei BP AsiaBizTech - 29-Jun-98.

⁷³ Garry Roday, The Internet and Social Control in Singapore, Pol. Sci. Q. Vol. 113, No. 1, Spring 1998.

⁷⁴ The Straits Times, September 27, 1996.

⁷⁵ Report of the National Internet Advisory Board 1997/1998, September 1998. <http://www.sba.gov.sg/work/sba/internet.nsf/>.

⁷⁶ Access to Information Act, C. A-1.

⁷⁷ Privacy Act, c. P-21.

⁷⁸ Privacy Commissioner of Canada; Information Commissioner of Canada.

⁷⁹ Telecommunications Act, 1993, c. 38, s. 39, s. 41.

⁸⁰ Bank Act, c. 46, ss. 242, 244, 459.

⁸¹ Insurance Companies Act, s. 489, s. 607.

⁸² Constitution of India, November 1949.

⁸³ National Task Force on IT & SD, Basic Background Report, 9th June 1998.

⁸⁴ The Constitution of the Republic of South Africa, Act 108 of 1996. Sections 14 and 32.

⁸⁵ Open Democracy Bill No. 67, 1998.

⁸⁶ See Rosario Imperiali d'Afflito, *European Union Directive on Personal Privacy Rights and Computerized Information*, 41 Vill. L. Rev 305 (1996).

⁸⁷ See Craig T. Beling, Note, *Transborder Data Flows: International Privacy Protections and the Free Flow of Information*, 6 B.C. Int'l & Comp. L. Rev. 591, 614-16 (1983). The Convention does not directly impose binding norms on signatories, but it requires nations to establish domestic data protection legislation. *Council of Europe Convention*, note 97, art. 4.1.

⁸⁸ How Do Public Attitudes On Privacy Vary Among Nations: A Comparative Analysis Of National Privacy Surveys Prepared for the Global Business Privacy Project of the Center for Social and Legal Research. Colin J. Bennett Associate Professor Department of Political Science University of Victoria Victoria, B.C. V8W 3P5, Canada First Draft, September 1996.

⁸⁹ Oversight Of The Privacy Act Of 1974: Hearings Before A Subcomm. Of The House Comm. On Government Operations, 98th Cong., 1st Sess. 226 (1983) (testimony of Ronald Plesser, former counsel to the Privacy Protection Study Commission). *see also* Schwartz, *supra* note 82, at 596 (noting that individuals seeking enforcement of their rights under Privacy Act "face numerous statutory hurdles, limited damages and scant chance to effect an agency's overall behavior").

⁹⁰ One example comes from a comparison of the treatment of tax information in Sweden and the United States. In Sweden, an individual's net income and tax deductions are public. Flaherty, *supra* note 2, at 146. In the United States, federal tax records are protected from disclosure by law. *See* 26 U.S.C. ' 6103 (1994).

⁹¹ One way to minimize privacy problems is to avoid collecting personal information. New technology may permit some activities to be conducted anonymously. Anonymity is not a complete solution. *See generally* Information And Privacy Commissioner (Ontario, Canada) & Registratiekamer (The Netherlands), *Privacy-Enhancing Technologies: The Path To Anonymity* (1995).

⁹² Another approach is to build into network operating systems protocols and procedures that define and perhaps even enforce the rights of participants. For example, some degree of privacy might be assured if the network automatically provided encryption of all communications and transactions. Network protocols can establish rules of practice that are the same as or perhaps even stronger than formal legal restrictions because it can be impossible for network users to avoid or evade the rules.

⁹³ There is precedent for the development of private law. *See, e.g.*, Michael T. Medwig, Note, *The New Law Merchant: Legal Rhetoric and Commercial Reality*, 24 Law & Pol'y Int'l Bus. 589, 589-90 (1993). The author comments:

⁹⁴ *The Philosophy Of George Santayana* 560 (Paul Arthur Schilpp ed., 2d ed. 1951).