ARTICLES

GLOBAL TRENDS IN PRIVACY PROTECTION: AN INTERNATIONAL SURVEY OF PRIVACY, DATA PROTECTION, AND SURVEILLANCE LAWS AND DEVELOPMENTS

by DAVID BANISAR AND SIMON DAVIES OF PRIVACY INTERNATIONAL†

TABLE OF CONTENTS

† David Banisar, Esq. is an attorney and writer in the Washington, DC area. He is Deputy Director of Privacy International (PI) and a Senior Fellow at the Electronic Privacy Information Center (EPIC). Simon Davies is Director General of Privacy International and a Visiting Fellow at the London School of Economics. Mr. Davies serves on the Professional Advisory Board of this publication. This article is based on *Privacy and Human Rights 1999: An International Survey of Privacy Laws and Developments*, which was written with support from the Open Society Institute and the EPIC Trust. Knowledgeable individuals from academia, government, human rights groups and other fields were asked to submit reports and information. Their reports were supplemented with information gathered from Constitutions, laws, international and national government documents, news reports, human rights reports and other sources. An electronic version of the full report and updates are available at the Privacy International web page at <http://www.privacyinternational.org/survey/>. Privacy International is a human rights group formed in 1990 as a watchdog on surveillance by governments and corporations. PI is based in London, UK and has an office in Washington, D.C. EPIC is a public interest group in Washington, D.C. that promotes privacy, free speech and freedom of information. More information on EPIC is available at <http://www.epic.org/>.

I. OVERVIEW

Privacy is a fundamental human right recognized in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional treaties. Privacy underpins human dignity and other values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age.

Nearly every country in the world recognizes a right of privacy in their constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. Most recently written constitutions such as South Africa's and Hungary's include specific rights to access and control one's personal information. In many of the countries where privacy is not explicitly recognized in the constitution, such as the United States (U.S.), Ireland and India, the courts have found that right in other provisions. In many countries, international agreements that recognize privacy rights such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights were adopted into law.

In the early 1970s, countries began adopting broad laws intended to protect individual privacy. Throughout the world, there is a general movement towards adopting comprehensive privacy laws that set a framework for protection. Most of these laws are based on the models introduced by the Organization for Economic Cooperation and Development and the Council of Europe.

In 1995, conscious both of the shortcomings of law, and the many differences in the level of protection in each of its States, the European Union (E.U.) passed a Europe-wide directive which will provide citizens

with a wider range of protections over abuses of their personal information.[1] The directive on the "Protection of Individuals with regard to the processing of personal data and on the free movement of such data" set a benchmark for national law. Each E.U. State must pass complementary legislation to incorporate this into their domestic laws.

The Directive also imposes an obligation on member States to ensure that the personal information relating to European citizens is covered by law when it is exported to, and processed in, countries outside Europe. This requirement has resulted in growing pressure outside Europe for the adoption of privacy laws. Nearly fifty countries now have comprehensive data protection or information privacy laws or are in the process of adopting them.

A. Threats to Privacy

The increasing sophistication of information technology with its capacity to collect, analyze and disseminate information on individuals introduced a sense of urgency to the demand for privacy legislation. Furthermore, new developments in medical research and care, telecommunications, advanced transportation systems and financial transfers dramatically increased the level of information generated by each individual. Computers linked together by high-speed networks with advanced processing systems can create comprehensive dossiers on any person without the need for a single central computer system. New technologies developed by the defense industry are spreading into law enforcement, civilian agencies, and private companies.

According to opinion polls, concern over privacy violations is now greater than at any time in recent history.[2] Uniformly, populations throughout the world express fears about encroachment on privacy, prompting an unprecedented number of nations to pass laws specifically protecting the privacy of their citizens. Human rights groups are concerned that much of this technology is being exported to developing countries that lack adequate protections. Currently, there are few barriers to the trade in surveillance technologies.

It is now common wisdom that the power, capacity and speed of information technology ("IT") is accelerating rapidly. The extent of privacy invasion, or certainly the potential to invade privacy, increases correspondingly. Beyond these obvious aspects of capacity and cost, there are a number of important trends that contribute to privacy invasion:

---

1. Council Directive 95/46/EC, 1998 O.J. (L024) (regarding the processing of personal data and on the free movement of such data).

2. Simon Davies, *Re-engineering the Right to Privacy: How Privacy has been Transformed from a Right to a Commodity*, *in* Technology and Privacy: The New Landscape 143 (Philip E. Agre & Marc Rotenberg eds., 1997).

GLOBALIZATION removes geographical limitations to the flow of data. The development of the Internet is perhaps the best known example of a global technology.

CONVERGENCE is leading to the elimination of technological barriers between systems. Modern information systems are increasingly inter-operable with other systems, and can mutually exchange and process different forms of data.

MULTI-MEDIA fuses many forms of transmission and expression of data and images so that information gathered in a certain form can be easily translated into other forms.

1. *Technology transfer and policy convergence*

The macro-trends outlined above had particular effect on surveillance in developing nations. In the field of information and communications technology, the speed of policy convergence is compressed. Across the surveillance spectrum: wiretapping, personal ID systems, data mining, censorship or encryption controls; it is the industrialized countries that invariably set a proscriptive pace.[3]

Governments of developing nations rely on First World countries to supply them with technologies of surveillance such as digital wiretapping equipment, deciphering equipment, scanners, bugs, tracking equipment and computer intercept systems. The transfer of surveillance technology from first to third world is now a lucrative sideline for the arms industry.[4]

According to a 1997 report, *Assessing the Technologies of Political Control,* commissioned by the European Parliament's Civil Liberties Committee and undertaken by the European Commission's Science and Technology Options Assessment office (STOA),[5] much of this technology is used to track the activities of dissidents: human rights activists, journalists, student leaders, minorities, trade union leaders, and political opponents. The report concludes that such technologies, which it describes as "new surveillance technology," can exert a powerful "chilling effect" on those who "might wish to take a dissenting view and few will risk exercising their right to democratic protest." Large-scale ID systems are also useful for monitoring larger sectors of the population. In the absence of meaningful legal or constitutional protections, such technology is inimi-

3. Simon Davies & Ian Hosein, *Liberty on the Line, in* LIBERATING CYBERSPACE (Liberty ed. 1998).

4. Privacy International, *Big Brother Incorporated: A Report on the International Trade in Surveillance Technology and its Links to the Arms Industry* (Nov. 1995) <http://www.privacyinternational.org/pi/reports/big_bro/>.

5. Europarl: Science and Technology Options Assessment ("STOA"), *Assessing the Technologies of Political Control* (Sept. 1998) <http://www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm>.

cal to democratic reform. It can certainly prove fatal to anyone "of interest" to a regime.

Government and citizens alike may benefit from the plethora of IT schemes being implemented by the private and public sectors. New "smart card" projects in which client information is placed on a chip in a card may streamline complex transactions. The Internet will revolutionize access to basic information on government services. Encryption can provide security and privacy for all parties. However, these initiatives will require a bold, forward looking legislative framework. Whether governments can deliver this framework depends on their willingness to listen to the pulse of the emerging global digital economy and to recognize the need for strong protection of privacy.

2. *Defining Privacy*

Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define and circumscribe.[6] Privacy has roots deep in history. The Bible has numerous references to privacy.[7] There was also substantive protection of privacy in early Hebrew culture, classical Greece and ancient China.[8] These protections mostly focused on the right to solitude. Definitions of privacy vary widely according to context and environment. In many countries, the concept has been fused with data protection, which interprets privacy in terms of managing personal information. Outside this rather strict context, privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs.[9] It can be divided into the following facets:

> *Information privacy*, involving the establishment of rules governing the collection and handling of personal data such as credit information and medical records;
>
> *Bodily privacy*, concerning the protection of people's physical beings against invasive procedures such as drug testing and cavity searches;
>
> *Privacy of communications*, covering the security and privacy of mail, telephones, email and other forms of communication; and
>
> *Territorial privacy*, concerning the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.

---

6. JAMES MICHAEL, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL AND COMPARATIVE STUDY 1 (1994).

7. RICHARD HIXSON, PRIVACY IN A PUBLIC SOCIETY: HUMAN RIGHTS IN CONFLICT 3 (1987). *See* BARRINGTON MOORE, PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY (1984).

8. *See supra* note 7.

9. SIMON DAVIES, BIG BROTHER: BRITAIN'S WEB OF SURVEILLANCE AND THE NEW TECHNOLOGICAL ORDER 23 (1996).

The lack of a single definition should not imply that the issue lacks importance. As one writer observed, "in one sense, all human rights are aspects of the right to privacy."[10]

Some historical viewpoints on privacy:

> In the 1890s, future U.S. Supreme Court Justice Louis Brandeis articulated a concept of privacy that urged that it was the individual's "right to be left alone." Brandeis argued that privacy was the most cherished of freedoms in a democracy, and he was concerned that it should be reflected in the Constitution.[11]

The Preamble to the Australian Privacy Charter provides, "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 . . . ." It also states, "Privacy is a key value which underpins human dignity and other key values such as freedom of association and freedom of speech. . . ." and "[p]rivacy is a basic human right and the reasonable expectation of every person."[12]

Alan Westin, author of the seminal 1967 work "Privacy and Freedom," defined privacy as the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others.[13]

According to Edward Bloustein, privacy is an interest of the human personality. It protects the inviolate personality, the individual's independence, dignity and integrity.[14]

According to Ruth Gavison, there are three elements in privacy: secrecy, anonymity and solitude. It is a state which can be lost, whether through the choice of the person in that state or through the action of another person.[15]

The Calcutt Committee in the UK said, "nowhere have we found a wholly satisfactory statutory definition of privacy." But the committee was satisfied that it would be possible to define it legally and adopted this definition in its first report on privacy:

> The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means

---

10. Fernando Volio, *Legal Personality, Privacy and the Family*, THE INTERNATIONAL BILL OF RIGHTS (Henkin ed. 1981).

11. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193-220 (1890).

12. AUSTRALIAN PRIVACY CHARTER GROUP, THE AUSTRALIAN PRIVACY CHARTER (University of New South Wales Law School 1994).

13. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

14. Edward Bloustein, *Privacy as an Aspect of Human Dignity*, 39 N.Y.U. L. REV. 971 (1964)

15. Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428 (1980).

or by publication of information.[16]

B. The Right to Privacy

Privacy can be defined as a fundamental, though not absolute, human right. The law of privacy can be traced as far back as 1361, when the English Justices of the Peace Act provided for the arrest of peeping toms and eavesdroppers.[17] In 1765, British Lord Camden, striking down a warrant to enter a house and seize papers wrote, "[w]e can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have."[18] Parliamentarian William Pitt wrote,

> 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 through 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.

In the centuries that followed, various countries developed specific protections for privacy. In 1776, the Swedish Parliament enacted the access to Public Records Act which required that all government-held information be used for legitimate purposes. In 1792, the Declaration of the Rights of Man and the Citizen declared that private property is inviolable and sacred. France prohibited the publication of private facts and set stiff fines for violators in 1858.[19] In 1890, American lawyers Samuel Warren and Louis Brandeis wrote a seminal piece on the right to privacy as a tort action describing privacy as "the right to be left alone."[20]

The modern privacy benchmark at an international level can be found in the 1948, Universal Declaration of Human Rights, which specifically protected territorial and communications privacy. Article 12 states:

> No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.[21]

---

16. Report of the Committee on Privacy and Related Matters Cmnd. 1102, p. 7 (1997) (Chairman David Calcutt, Q.C.).

17. Michael, *supra* note 7, at 15.

18. Entick v. Carrington, 1558-1774 All E.R. Rep. 45.

19. Judgment of June 16, 1858, Trib. pr. inst. de la Seine, 1858 D.P. III 62 (Fr.) (affaire Rachel); *see* Jeanne M. Hauch, *Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris*, 68 Tul. L. Rev. 1219 (1994).

20. *See* Warren & Brandeis, *supra* note 12, at 193.

21. Human Rights Web, *U.N. Universal Declaration of Human Rights*, July 6, 1994 (ed. Jan. 27, 1997).

Numerous international human rights covenants give specific reference to privacy as a right. The International Covenant on Civil and Political Rights (ICCPR),[22] the UN Convention on Migrant Workers[23] and the UN Convention on the Rights of the Child[24] adopt the same language.

On the regional level, various treaties can make these rights legally enforceable. Article 8 of the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms[25] states:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others.

The Convention created the European Commission of Human Rights and the European Court of Human Rights to oversee enforcement. Both were particularly active in the enforcement of privacy rights and have consistently viewed Article 8's protections expansively and the restrictions narrowly.[26] The Commission found in its first decision on privacy:

> For numerous Anglo-Saxon and French authors, the right to respect "private life" is the right to privacy, the right to live, as far as one wishes, protected from publicity .... In the opinion of the Commission, however, the right to respect for private life does not end there. It comprises also, to a certain degree, the right to establish and develop relationships with other human beings, especially in the emotional field for the development and fulfillment of one's own personality.[27]

The Court has reviewed member states' laws and imposed sanctions on several countries for failing to regulate wiretapping by governments and private individuals.[28] It also reviewed cases of individuals' access to their personal information in government files to ensure that adequate

---

22. *International Covenant on Civil and Political Rights*, U.N.T.S. No. 14668, vol. 999, at 171 (1976).

23. *International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families*, G.A. Res. 158, U.N. GAOR, 45th Sess., Art. 14, U.N. Doc. A/RES/45/158 25 (1991).

24. *Convention on the Rights of the Child*, U.N. GAOR, 44th Sess, 61st plen. mtg., Annex, Art. 16, U.N. Doc A/RES/44/25 (1989).

25. CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS Rome, 4.XI.1950, *available at* <http://www.coe.fr/eng/legaltxt/5e.htm>.

26. Nadine Strossen, *Recent U.S. and Intl. Judicial Protection of Individual Rights: A Comparative Legal Process Analysis and Proposed Synthesis*, 41 HASTINGS L.J. 805 (1990).

27. X v. Iceland, 5 Eur. Comm'n H.R. Dec. & Rep. 86, 87 (1976).

28. Case of Klass and Others, 28 Eur. Ct. H.R. (Ser. A) (Judg. of Sept. 6, 1978) (1979); Malone v. Commissioner of Police, 2 All E.R. 620 (1979); *see* Note, *Secret Surveillance and the European Convention on Human Rights*, 33 STAN. L. REV. 1113, 1122 (1981).

procedures exist.[29] It has expanded the protections of Article 8 beyond government actions to those of private persons where it appears that the government should have prohibited those actions.[30] Presumably, under these combined analyses, the court could order the imposition of data protection laws if data was improperly processed to the detriment of the person who was subject of the data.[31]

Other regional treaties are also beginning to be used to protect privacy. Article 11 of the American Convention on Human Rights sets out the right to privacy in terms similar to the Universal Declaration.[32] In 1965, the Organization for American States proclaimed the American Declaration of the Rights and Duties of Man, which called for the protection of numerous human rights including privacy.[33] The Inter-American Court of Human Rights began to address privacy issues in its cases.

C. The Evolution of Data Protection

Interest in the right of privacy increased in the 1960s and 1970s with the advent of IT. The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information. In many countries, new constitutions reflect this right. The genesis of modern legislation in this area can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970. This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977), and France (1978).[34]

Two crucial international instruments evolved from these laws. The Council of Europe's (COE) 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[35] and the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data

---

29. Leander Case, Eur. Ct. H.R., No. 10/1985/96/144 (Judg. of Mar. 26, 1987).

30. *Id.* at 848 – 49.

31. Rolv Ryssdal, *Data Protection and the European Convention on Human Rights in Council of Europe Data Protection, Human Rights and Democratic Values*, XIII Conference of the Data Commissioners 41-43 (1992).

32. *American Convention on Human Rights*, Inter-American Commission on Human Rights, Nov. 22, 1969, O.A.S. Treaty Series No. 36, at 1, O.A.S. Off. Rec. OEA/Ser. L/V/II.23 dec rev. 2 (entered into force July 18, 1978).

33. *American Declaration of the Rights and Duties of Man*, Inter-American Commission on Human Rights, adopted by the Ninth Conference of American States, 1948, O.A.S. Off. Rec. OEA/Ser/L./V/I.4 Rev (1965).

34. For an excellent analysis of these laws, see David Flaherty, Protecting Privacy in Surveillance Societies (1989).

35. Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Strasbourg, 1981, *available at* <http://www.coe.fr/eng/legaltxt/108e.htm>.

Flows of Personal Data[36] articulate specific rules covering the handling of electronic data. The rules within these two documents form the core of the Data Protection laws of dozens of countries. These rules describe personal information as data that are afforded protection at every step from collection to storage and dissemination.

The expression of data protection in various declarations and laws varies in degree. All of the declarations and laws require that personal information must be:

- obtained fairly and lawfully;
- used only for the original specified purpose;
- adequate, relevant and not excessive to purpose;
- accurate and up to date;
- accessible to the subject;
- kept secure; and
- destroyed after its purpose is completed.

These two agreements have had a profound effect on the enactment of laws around the world. Over twenty countries have adopted the COE convention and another six have signed it but have not yet adopted it into law. The OECD guidelines are also widely used in national legislation, even outside the OECD countries.

1. *Reasons for Adopting Comprehensive Laws*

There are three major reasons for the movement towards comprehensive privacy and data protection laws. Many countries are adopting these laws for one or more of the following reasons:

To remedy past injustices. Many countries, especially in Central Europe, South America and South Africa, are adopting laws to remedy privacy violations that occurred under previous authoritarian regimes.

To promote electronic commerce. Many countries, especially in Asia, but also Canada, have developed or are currently developing laws in an effort to promote electronic commerce. These countries recognize consumers are uneasy with their personal information being sent worldwide. Privacy laws are being introduced as part of a package of laws intended to facilitate electronic commerce by setting up uniform rules.

To ensure laws are consistent with Pan-European laws. Most countries in Central and Eastern Europe are adopting new laws based on the Council of Europe Convention and the European Union Data Protection Directive. Many of these countries hope to join the European Union in the near future. Countries in other regions, such as Canada,

36. Organization for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data* (Paris, 1981).

are adopting new laws to ensure that trade will not be affected by the requirements of the E.U. Directive.

2. *The European Telecommunications Directive and the European Data Protection Directive*

In the past three years, the European Union (E.U.) enacted two directives providing citizens with a wider range of protections over abuses of their data. The Telecommunication Directive and the Data Protection Directive set a baseline common level of privacy which not only reinforce current data protection law, but extend it to establish a range of new rights. The Data Protection Directive sets a benchmark for national law that will harmonize data protection law throughout the European Union.[37] Each E.U. State was required to enact complementary legislation by October 1998, though it is more likely that not all will complete the process until the end of 2000. The Telecommunications Directive[38] establishes specific protections covering telephone, digital television, mobile networks and other telecommunications systems.

Several principles of data protection are strengthened under the Directives, the right to know where the data originated, the right to have inaccurate data rectified, a right of recourse in the event of unlawful processing and the right to withhold permission to use data in some circumstances. For example, individuals will have the right to opt-out free of charge from being sent direct marketing material. The Data Protection Directive contains strengthened protections over the use of sensitive personal data relating, for example, to health or finances. In the future, the commercial and governmental use of such information will generally require "explicit and unambiguous" consent of the data subject.

The key concept in the European model is "enforceability." The E.U. is concerned that data subjects have rights that are enshrined in explicit rules, and that they can go to a person or an authority that can act on their behalf. Every E.U. country will have a Privacy Commissioner or agency that enforces the rules. It is expected that the countries with which Europe does business will be required to have a similar level of oversight.

The Directive imposes an obligation on member States to ensure that the personal information relating to European citizens is covered by

37. Council Directive 95/46/EC, 1995, *available at* <http://www.odpr.org/restofit/Legislation/Directive/Directive_Contents.html>. The directive, issued by the European Parliament and by the Council on 24 Oct. 1995, addresses the protection of individuals with regard to the processing of personal data and on the free movement of such data.

38. Council Directive 97/66/EC, 1997, *available at* <http://www2.echo.lu/legal/en/dataprot/protection.html>. The directive, issued by the European Parliament and of the Council on 15 Dec. 1997, concerns the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector.

law when it is exported to, and processed in, countries outside Europe.[39] This requirement has resulted in growing pressure outside Europe for the passage of privacy laws. Those countries that refuse to adopt meaningful privacy law may find themselves unable to conduct transactions involving certain types of information flows with Europe, particularly if the transactions involve sensitive data.

The Telecommunications Directive imposes wide-ranging obligations on carriers and service providers to ensure the privacy of users' communications, including Internet-related activities. The new rules will cover areas that until now have fallen between the cracks of data protection laws. Access to billing data will be severely restricted, as will marketing activity. Caller ID technology must incorporate an option for per-line blocking of number transmission. Information collected in the delivery of a communication must be purged once the call is completed.

D. Models of Privacy Protection

There are currently several major models for privacy protections. Depending on their application, these models can be complimentary or contradictory. In most of the countries reviewed in the survey, several models of privacy protections are used simultaneously. In the countries that protect privacy the most, all of the models work together to ensure privacy protection.

1. *Comprehensive laws*

In many countries around the world, there is a data protection law that governs the collection, use and dissemination of personal information by both the public and private sectors. This is the preferred model for most countries adopting data protection law. It is also the model favored by Europe to ensure compliance with its new data protection regime. In most of these countries, there is also an official or agency that oversees enforcement of the act. This official, known variously as a Commissioner, Ombudsman or Registrar, monitors compliance with the law and conducts investigations into alleged breaches. In some cases the official can find against an offender. The official is also responsible for educating the public and acts as international liaison in data protection and data transfer. However, the powers of the commissions vary greatly and many report a serious lack of resources to adequately enforce the laws. A variation of these laws, which is described as a *co-regulatory model*, is

39. Article 25 of the Directive stipulates that in many circumstances, the level of protection in the receiving country must be "adequate" - an expression which is widely accepted to mean "equivalent." Article 26 lays out certain options for transferring data out of Europe in circumstances where the level of protection is not deemed adequate. These include consent and contracts.

currently being adopted in Canada and Australia. Under this approach, industry develops enforceable standards for the protection of privacy that are enforced by the industry and overseen by a privacy agency.

2. *Sectoral Laws*

Some countries such as the U.S. have avoided general data protection rules in favor of specific sectoral laws governing, for example, video rental records or financial privacy. In such cases, enforcement is achieved through a range of mechanisms. A major drawback with this approach is that it requires that new legislation be introduced with each new technology so protections frequently lag behind. There is also the problem of the lack of an oversight agency. The lack of legal protections for medical and genetic information in the U.S. is a striking example of the limitations of these laws. In many countries, sectoral laws are used to complement comprehensive legislation by providing more detailed protections for certain categories of information, such as telecommunications, police files or consumer credit records.

3. *Self Regulation*

Data protection can also be achieved - at least in theory - through various forms of self-regulation, in which companies and industry bodies establish codes of practice. However, these efforts were disappointing, with little evidence that the aims of the codes are regularly fulfilled. Adequacy and enforcement are the major problem with these approaches. Industry codes in many countries tend to provide only weak protections and lack enforcement. This is currently the policy promoted by the governments of U.S., Japan, and Singapore.

4. *Technologies of Privacy*

Privacy protection has moved into the hands of individual users with the recent development of commercially available *technology-based systems.* Users of the Internet and of some physical applications can employ a range of programs and systems that will ensure varying degrees of privacy and security of communications. These include encryption, anonymous remailers, proxy servers, digital cash and smart cards. Questions remain about security and trustworthiness of these systems. Recently, the European Commission evaluated some of the technologies and stated that the technological tools would not replace a legal framework, but could be used to compliment existing laws.[40]

40. Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), *available at* <http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp11en.htm>.

E. Continuing Problems

Even with the adoption of legal and other protections, violations of privacy remain a concern. In many countries, laws have not kept up with the technology, leaving significant gaps in privacy protections. In other countries, law enforcement and intelligence agencies were given significant exemptions to privacy laws. Finally, without adequate oversight and enforcement, the mere existence of a law may not provide individuals with adequate protection.

There are widespread violations of laws relating to the surveillance of communications, even in the most democratic of countries. The U.S. State Department's annual review of human rights violations found that over 90 countries illegally monitor the communications of political opponents, human rights workers, journalists and labor organizers. In 1996, a French government commission estimated that there were over 100,000 illegal wiretaps conducted by private parties, many of these on behalf of government agencies. There were protests in Ireland after it was revealed that the UK was monitoring all UK/Ireland communications from a base in Northern England. In Japan, police were recently fined 2.5 million yen for illegally wiretapping members of the Communist Party. The Echelon system is used by the U.S., UK, Australia, Canada and New Zealand to monitor communications worldwide.

Police services, even in countries with strong privacy laws, still maintain extensive files on citizens for political purposes not accused or even suspected of any crime. There are currently investigations in Sweden and Norway, two countries with the longest history of privacy protection for intelligence and police files. In Switzerland, a scandal over secret police spying led to the enactment of their data protection act. In many former Eastern Bloc countries, there are still controversies over the disposition of the files of the secret police.

Companies regularly flaunt the data protection laws, collecting and disseminating personal information. In the U.S., even with the longstanding existence of a law on consumer credit information, companies still make extensive use of such information for marketing purposes and banks sell customer information to marketers. In other countries, inadequate security has resulted in the accidental disclosure of thousands of customers' records.

II. COUNTRY REPORTS

Argentine Republic

Articles 18 and 19 of the Argentine Constitution protect the privacy of individuals. Article 43, enacted in 1994, provides a right of Habeas