The Sedona Conference Journal

Volume 2 2001

Protecting Privacy through Government Regulation

Sarah Andrews

Recommended Citation: Sarah Andrews, *Protecting Privacy through Government Reguation*, 2 SEDONA CONF. J. 1 (2001).

Copyright 2001, The Sedona Conference

For this and additional publications see:
https://thesedonaconference.org/publications

PROTECTING PRIVACY THROUGH GOVERNMENT REGULATION

Sarah Andrews,
E.P.I.C., Washington, D.C.

INTRODUCTION

Although concerns over the loss of personal privacy appear to have risen to the forefront of public debate in the last number of years, the need to protect individuals against unwarranted invasions into their private lives is by no means a "new" issue. In fact, the topic has been contemplated for millennia. For example, the laws and social practices in ancient Greece and Rome recognized that individuals need to distinguish between their private and public lives in order to participate fully in society;[1] the Bible contains many references to the value of privacy;[2] a doctrine in Jewish law protects individuals from the harm of unwanted surveillance or even the possibility of unwanted surveillance.[3] The concept of special protections for family life and the inviolability of the home is similarly time-honored. The common cliché that *"a man's home is his castle*" traces its roots back to a series of controversial search and seizure cases in the UK in the 1760s.[4] In general these kinds of protections were guaranteed on moral and social justifications. Over the years, however, the right to privacy has become "posited" in our legal system.[5]

At the international and regional level, privacy is identified as a fundamental human right in Universal Declaration of Human Rights (1948)[6]; the International Covenant on Civil and Political Rights (1976);[7] the American Convention on Human Rights (1978);[8] and the European Convention for the Protection of Human Rights and Fundamental Freedoms (1953).[9] The passage of these kinds of treaties in the second half of the twentieth century was largely a response to the atrocities committed during World War Two. The reliance of Nazi Germany on centralized registries in its persecution of the Jews and occupation of Europe painfully highlighted the potential threats of misuse of personal information and the need to protect privacy at the highest levels.[10]

At the national level, the legal right to privacy is included in the constitution of most countries.[11] In many this is framed as a right to respect for the home, family life and private correspondence. In others, the right to control the collection and dissemination of personal information is expressly set out. In others still, particularly in Latin American

1 Richard C. Turkington & Anita Allen, *Privacy Law Cases and Materials* 3-22 (1999); Joel Reidenberg, *Setting Standards for Fair Information Practices in the U.S. Private Sector*, 80 Iowa L. Rev. 497, 497-8 (1995)
2 Turkington & Allen, id., 3-22
3 Jeffrey Rosen, *The Unwantd Gaze: The Destruction of Pivacy in America* 18-19 (2000)
4 Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 Va. L. Rev. 869 cited in ROSEN, id., 27-31; David Banisar, *Privacy and Human Rights: An International Survey of Privacy Laws and Developmnts* 5 (2000).
5 Howard B. Radest, *The Public and the Private: An American Fairy Tale*, 89 Ethics 280, 280-88 (1979) reproduced in Turkington & Allen, supra n.1 at 11, says that notions of privacy whether based in liberal theory or natural law philosophies have become "demythologized" by positive law.
6 Article 12 provides that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence."
7 Part III, article 17 specifically guarantees "[t]he right to privacy."
8 Article 11 provides that:
"1. Everyone has the right to have his honor respected and his dignity recognized.
2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
3. Everyone has the right to the protection of the law against such interference or attacks."
9 Article 8 protects "[t]he right to respect for private and family life, the home and correspondence."
10 Stephanie Perin et al., *The Personal Information Potection and Electronic Documnts Act: An Annotatd Guide* 2 (2001)
11 For an overview of privacy laws and practices around the world see Banisar, supra n.4.

countries, a right for individuals to access all information held about themselves is included.[12] Even in those constitutions where there is no express reference to privacy, courts have generally been able to imply its protection in other individual rights provisions. In the U.S., for example, although it does not specifically guarantee a right to privacy, the Fourth Amendment to the Constitution forms the basis of the principal claim to freedom from government invasion.[13] In conjunction with the Fifth Amendment prohibition on self-incrimination, it has been used time and time again to prevent the seizure of private papers and unlawful government surveillance.[14] In addition, other provisions in the Bill of Rights have been invoked to establish a right to privacy in areas such as contraception;[15] abortion;[16] personal and sensitive information;[17] marriage and family life;[18] freedom of association;[19] and freedom of speech.[20]

Within common law systems, the emergence and subsequent evolvement of the "Privacy Tort" has also greatly increased the protection of individual privacy. The origins of this cause of action are so firmly grounded in U.S. jurisprudence that it is sometimes referred to as the "American Tort."[21] The crucial development in this area came with the publication in 1890 of "The Right to Privacy," a law review article by Supreme Court Justice to be, Louis Brandeis, and his law partner, Samuel Warren. They argued that due to *"[r]ecent inventions and business methods*," the time had come to secure within the law, "*the next step which must be taken for the protection of the person…..[namely] the right to be let alone*."[22] By 1939, protection for the right to privacy was expressly recognized in the First Restatement on Tort.[23] By 1960 over 300 cases involving privacy were identified as having been brought before the appellate courts.[24]

The common law torts for breach of privacy fall into four categories: intrusion upon seclusion; appropriation of name or likeness; publicity given to private life; and publicity placing persons in false light.[25] While these protections work well for some aspects of privacy invasion, they are not all encompassing. For example, the right to respect for one's personal information, or information privacy, does not fit squarely within any of these four categories.[26] As we have seen, this realization and the need to address the increasing sophistication and pervasiveness of computer technology being developed throughout the 20th century led to the protection of privacy in international treaties. But it also led to the emergence of a new approach to privacy protection at national levels. In response to calls

12 This right, known as the right of "Habeas Data" is a relatively new development. For more information see, Andres Guadamuz, *Habeas Data: The Latin-American Response to Data Protection*, 2000 (2) Journal of Information, Law and Technology (JILT), available at http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html.

13 It states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…"

14 *See*, e.g. *Boyd v. United States*, 116 U.S. 616 (1886) (holding that an individual can not be compelled by government forces to disclose private documents); dissent of Justice Brandeis in *Olmstead v. United States*, 277 U.S. 438 (1928) (stating that wire-tapping was an unlawful invasion of privacy); *Berger v. New York* 388 U.S. 41 (1967) and *Katz v. United States*, 389 U.S. 347 (1976) (building on the Brandeis dissent, these two cases established the fundamental constitutional right to information privacy and freedom from electronic surveillance)

15 *Griswold v. Connecticut*, 381 U.S. 479 (1965) (relying on the Due Process Clause of the Fourteenth Amendment and additional rights guarantee in the Ninth Amendment , the Supreme Court held that prohibitions on contraceptives are unreasonable invasions of privacy and home life).

16 *Roe v. Wade*, 410 U.S. 113 (1973) (holding that statues criminalizing abortion violates a woman's right to privacy and autonomy contrary to the Fourteenth Amendment).

17 A number of cases indicate that a constitutional right to information privacy, independent of the Fourth Amendment, exists based on the concept of "liberty" in the Fifth and Fourteenth Amendments. *See,* e.g., *Nixon v. Administrator of Gen. Services.*, 433 U.S. 425 (1977); *Whalen v. Roe,* 429 U.S. 589 (1977): *United States v. Westinghouse*, 638 F. 2d 570 (3d Cir. 1980); *Woods v. White*, 689 F. Supp. 874 (W.D. Wis,. 1988)

18 *Loving v. Virginia*, 388 U.S. 1 (1967) (striking down Virginia laws prohibiting interracial marriages as an undue encroachment on the freedom to marry and in violation of the Equal Protection Clause.)

19 *NAACP v. Alabama*, 37 U.S. 449 (1958) (holding that the First Amendment includes a right to freely associate and to maintain privacy in those associations and therefore protects members of a political group from being forced to disclosing their members, names to government.

20 *McIntyre v. Ohio Elections Committee*, 514 U.S. 334 (1995) (holding that the First Amendment right to free speech includes the right to speak anonymously).

21 Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 Stan. Tech. L. Rev.1, par 26

22 Samuel D. Warren & Louis Brandeis, *The Right of Privacy*, 4 Harv. Law Rev. 193 , 193-4 (1890)

23 Turkington & Allen, supra n.1 at 23.

24 Id., at 24.

25 These elements are embodied in the Second Restatement of Torts, Sections 652B, C, D, and E. They were first identified by Dean William Prosser in *Privacy*, 48 Calif. L. Rev. 383, 388-9 (1960), reproduced in Turkington & Allen, supra n.1 at 59.

26 Reidenberg, supra n.1 at 503 analyses each of the four prongs of the common law tort and concludes that "[I]n isolation" not one of them provides a "broad restriction on the circulation and treatment of personal information." Moreover, he says, even in combination these torts can not "offer more than a small set of targeted restrictions on information flows." For an analysis of the "weakness" of the privacy tort to address privacy on the Internet, see Paul Schwartz, *Beyond Lessig's Code For Internet Privacy: Cyberspace Filters, Privacy Control and Fair Information Practices*, 4 Wisconsin Law Review, 743, 777-8 (2000)

from privacy and human rights advocates for measures placing restrictions on the collection, storage and dissemination of personal information, throughout the late 1960s and 1970s, governments began to introduce specific laws on information privacy.

These laws, known as data protection laws, have now become a central feature of privacy law. This paper examines their development and implementation around the world with a particular focus on the lagging protections in the current U.S. system. The aim is to assess the efficacy of the different models that have been put in place to address new challenges posed by computerized record keeping systems. Section I looks at the development of the principles of data protection. Section II examines the implementation of these principles around the world. Finally, using the recent conflict between the U.S. and the EU as an example, section III explores the problems that can arise from different approaches to what is essentially a global issue.

I. DEVELOPMENT OF DATA PROTECTION PRINCIPLES

Today, most developed nations around the world have either passed or proposed data protection laws.[27] Typically, these laws implement principles known as Fair Information Practices for the processing of all kinds of information. Fair Information Practices grant consumers specific rights over their personal information enforceable against the public and private sectors. They generally require that personal information must be: obtained fairly and lawfully; used only for the original specified purpose; reliable and not excessive to purpose; accurate and up to date; accessible to the subject; and securely stored.

The term "Fair Information Practices" was first coined by a U.S. study group. This group was set up by the Department of Health, Education and Welfare prior to the passage of the Privacy Act in 1974. In 1973 they published a report on *Records, Computers and the Rights of Citizens*[28] that identified five key principles to be respected in any information-keeping system:

- There must be no personal-data record-keeping system whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent the misuse of the data.[29]

They recommended the "*enactment of legislation establishing a Code of Fair Information Practice"* that would implement each of these five principles and be applied to all automated personal data systems. They advised that this Code:

- should define "fair information practice" as adherence to specified safeguard requirements

27 *See* generally, Banisar, supra n.4.
28 Department of Health, Education and Welfare, "*Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*" (Washington DC, 1973)
29 Id., at 41.

- should prohibit violation of any safeguard requirement as an "unfair information practice"
- should provide that an unfair information practice be subject to both civil and criminal penalties
- should provide for injunctions to prevent violation of any safeguard requirement
- should give individuals the right to bring suits for unfair information practices[30]

Furthermore, they recommended that each time a new or expanded personal data system is proposed, the administrators of that system carefully consider the need for and purpose of the system. In particular they recommended a number of questions to be asked such as:

- What purposes will be served by the system and the data to be collected?
- How might the same purposes be accomplished without collecting these data?
- If the system is an administrative personal data system, are the proposed data items limited to those necessary for making required administrative decisions about individuals as individuals?
- Is it necessary to store individually identifiable personal data in computer-accessible form, and, if so, how much?
- Is the length of time proposed for retaining the data in identifiable form warranted by their anticipated uses?"[31]

The Code of Fair Information Practices was a landmark development in the data protection debate and marked a major turning point in the development of laws worldwide.[32] The principles were mirrored at the international level. In 1981 the Council of Europe issued a convention on data protection.[33] It was the first binding international instrument to protect individuals against abuses in the collection and processing of their personal data. Consistent with the U.S. code of Fair Information Practices, this convention sets out that all data undergoing automatic processing must be:

- obtained and processed fairly and lawfully;
- stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are stored;
- accurate and, where necessary, kept up to date;
- preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[34]

Beyond this, it prohibits the processing of "sensitive" data (including data on a person's race, politics, health, religion, sexual life, and criminal record) in the absence of proper legal safeguards.[35] It implements the right of individuals to access and, if necessary, correct information concerning them[36] and also includes language to limit the transborder flow of personal data to States without "equivalent protection."[37]

---

30 Id., at 50.
31 Id.
32 Robert Gellman, *Does Privacy Law Work*, in *Technology and Privacy: The New Landscape* 196 (Philip E. Agre & Marc Rotenberg eds., 1998) (noting, however, that this does not mean that the Privacy Act has been particularly effective in practice. "There is a big difference," he says, "between adopting good policies and implementing them well.")
33 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108, Strasbourg, 1981 available at <http://conventions.coe.int >.
34 Article 5, id.
35 Article 6, id.
36 Article 8, id.
37 Article 12, id.

At the same time, the Organization for Economic Cooperation and Development (OECD) issued important guidelines on privacy and data protection.[38] Although resolutions of the OECD do not form binding international law, they are highly influential and provide clear principles for Member States when developing national policies. These guidelines set out eight principles to be regarded as "minimum standards" for the processing of data by both the private and the public sectors:

- The Collection Limitation Principle (limiting, and requiring consent for, the collection of personal information)
- The Data Quality Principle (ensuring the relevance and accuracy of data)
- The Purpose Specification Principle (specifying the purpose of the information collection)
- The Use Limitation Principle (prohibiting use for unrelated purposes)
- The Security Safeguards Principle (safeguarding the security of information)
- The Openness Principle (ensuring transparency in the collection process)
- The Individual Participation Principle (providing access for the data subject)
- The Accountability Principle (enforcing the principles effectively)

Together, these different articulations of Fair Information Practices had a profound effect on the introduction of data protection laws around the world and for a time at least it appeared that there was international convergence in policies towards information privacy.[39]

II. IMPLEMENTATION

In the U.S. the Fair Information Practice principles were directly incorporated into the Privacy Act of 1974, which governs the public sector collection and use of personal information.[40] The principles of notice;[41] consent;[42] purpose and use limitation;[43] reliability, relevancy and accuracy;[44] access[45]; and security[46] were clearly set out and civil and criminal penalties[47] established for their violation. In Europe, signatories to the Council of Europe convention and the OECD guidelines quickly began ratifying their provisions and by the early 1990s Austria, Belgium, the Czech Republic, Denmark, Finland, France, Germany, Hungary, Iceland, Ireland, Luxembourg, the Netherlands, Norway, Portugal, Spain, Switzerland, and the United Kingdom had comprehensive data protection laws in place.[48] Meanwhile, in non-European OECD member countries, such as Australia, Canada, Japan,

38 OECD, "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" Paris, 1981. http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.

39 Colin Bennet, *Regulating Privacy: Data Protection and Public Policy in Europe and The United States* 222 (1992) cited in TECHNOLOGY AND PRIVACY supra n. 32 at 100. Bennet suggests, however, that for many countries this convergence had less to do with actual concern for privacy protection than with political motives. He states: "For the pioneers, the United States and Sweden, the convergence resulted from independent and indigenous analyses that traveled along the same learning curve and arrived at the same conclusion. For West Germany and other countries such as Canada, France, Norway, Denmark and Austria that legislated in the late 1970s, the convergence slowed from the mutual process of lesson drawing within an international policy community. For Britain and other laggards such as the Netherlands, Japan, and Australia, the convergence has resulted from the pressure to conform to international standards mainly for commercial reasons."

40 Public Law 93-579.

41 5 U.S.C. Section 552a (e)(3) requires agencies maintaining a system of records to disclose to individuals: the authority under which they are requesting information and whether the disclosure of information is mandatory or voluntary; the principal purposes and routine uses of the information; and the consequences of not providing the requested information. Under 5 U.S.C. Section 552a (e)(4) these agencies are further required to publish a notice in the Federal Register revealing the existence and details of the system of records.

42 Subject to certain exceptions, 5 U.S.C. Section 552a (b) prohibits the disclosure of records to any third party "except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."

43 5 U.S.C. Section 552a (e)(1) requires agencies to limit collection of information to that which is "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."

44 5 U.S.C. Section 552a (e)(5)& (6) records are to be maintained with "accuracy, relevance, timeliness and completeness."

45 5 U.S.C. Section 552a (d) sets out a right of access for the individual including the right to review, copy, and amend the record.

46 5 U.S.C. Section 552a (e)(10) requires agencies to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

47 5 U.S.C. Section 552a (g) provides a right of private action for individuals including the right to monetary damages and attorney's fees. 5 U.S.C. Section 552a (i) sets a criminal penalty of $5,000 for wrongfully disclosing information, for failing to meet the notice requirements of Section 552a (4), or for requesting or obtaining information under false pretences.

48 The convention was open for signature by Council of Europe member States and for accession by non-member States. It has now been signed by thirty-one countries and ratified in 21 of those countries. *See*, Council of Europe, Chart of signatures and Ratifications for ETS No. 108, <http://conventions.coe.int>.

Korea and New Zealand, new data protection laws to reflect the 1980 Privacy Guidelines were also introduced.[49]

However, while there may have been general agreement on the nature of the principles, a clear divergence among countries, and particularly between the U.S. and Europe, emerged in terms of scope of implementation.[50] At the European level, the data protection laws being introduced were comprehensive in nature and binding both on the private and the public sectors. The introduction in 1995 of the EU Data Protection Directive consolidated this approach.[51] This Directive sought to harmonize national laws within the European Union in order to ensure the free flow of information across the internal market. It set out basic, standardized protections based on Fair Information Practices, which not only reinforced existing data protection laws but also extended them to create new rights. Like the Council of Europe Convention it recognized that sensitive information, such as medical, financial, sexual and other information, needed extra protections within the law. A requirement of "explicit and unambiguous" consent was set out for the processing of such information.[52] Finally the Directive regulated the transborder flow of information by providing that personal data could only be exported to a country outside of Europe if that country "ensures an adequate level of protection."[53]

This approach was not followed by the United States, where, as we have seen, the Privacy Act only applies to the public sector. It was also initially rejected in Australia, Canada and Japan, where the early data protection laws were only applicable to government processing of information. However, Australia and Canada have both recently extended data protection laws beyond the government and a similar bill is pending in Japan.[54] Today, therefore, the U.S. stands alone in opposing the implementation of comprehensive legislation for the private sector.

The U.S. approach is instead one of self-regulation and sectoral protections for privacy in the private sector. Sectoral laws target only narrow areas of the marketplace at a time. They are issued from time to time in response to new technologies or when particular problems or bad practices appear ubiquitous across an entire industry.[55] For example, the Family Educational Rights and Privacy Act 1974[56] regulates the treatment of student records by educational agencies and institutions. The Cable Communications Policy Act 1986[57] sets out strong protections for cable subscribers' personal information. The Video Privacy Protection Act 1988[58] extends similar protections to consumers of video tape service providers as are afforded to cable consumers. The Telephone Consumer Protection Act 1991[59] protects consumers from unwanted telemarketing calls. The Driver's Privacy Protection Act 1994[60] restricts the disclosure of personal information from State motor vehicle records. The Telecommunications Act 1996[61] requires telecommunications carriers to keep customer information confidential. The Children's Online Privacy Protection 1998[62]

---

49 OECD, *Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks*, DSTI/ICCP/REG(98)12/FINAL, 11 May 1999 available at <http://www.olis.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg(98)12-final>.

50 For an excellent study of the early implementation of data protection laws in the U.S., Canada, Sweden, France and Germany see David H. Flaherty, *Protecting Privacy in Surveillance Societies*, (1989)

51 Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) 31 (Nov. 23, 1995) available at < http://europa.eu.int/comm/internal_market/en/media/dataprot/law/index.htm>

52 Article 8, id.

53 Article 25, id.

54 In Australia, the Privacy Amendment (Private Sector) Bill 2000 was approved by the Parliament and signed into law in December 2000. <http://www.law.gov.au/privacy/royalinfo.html 2002>. In Canada, the Personal Information Protection and Electronic Documents Act was passed in April 2000 and came into effect on January 1, 2001. http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html. In Japan, the government approved a data protection bill for the collection of personal information for commercial use, on March 27, 2001. It hopes to have the bill passed into law in the current session and to have it in force by 2003. See, *Bill on data protection approved by Cabinet*, March 28, 2001, Japan Times available at <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20010328a3.htm>.

55 See generally "The Privacy Law Sourcebook 2000: United States Law, International Law, and Recent Developments," Marc Rotenberg (EPIC 2000).

56 Public Law 93-380

57 Public Law 98-549

58 Public Law 100-618

59 Public Law 102-243

60 Public Law 103-322

61 Public Law 104-104

62 Public Law 105-277

limits the collection of personal information, by website operators, from children under the age of thirteen. The Right to Financial Privacy Act 1978[63] and the Financial Services Modernization Act 1999[64] protect the privacy of consumers' financial records. Finally, the recently enacted medical regulations (HIPPA regulations) protect the confidentiality of individuals, medical records.[65] While these privacy laws are useful to provide more detailed protections for certain categories of information, the underlying flaw of a sectoral approach to privacy protection is that the laws continually need to be updated as new technologies give rise to unanticipated practices. Without a backdrop of a comprehensive privacy law, U.S. individuals cannot be assured of privacy protection on an on-going basis.[66]

Even less can be said of a self-regulatory regime for privacy protection. This has been the official approach of the U.S. government for Internet privacy since the early 1990s and is strongly backed by the corporate sector. Under such a scheme businesses voluntarily agree to abide by a set of good principles. The idea is to avoid "heavy-handed" regulation and allow competitive forces within the marketplace to respond to consumer demands. The fundamental flaw in this method is that there is no real oversight and enforcement. Even when companies sign on to a "seal" program of a third-party body, bad practices most often go unpunished. In many cases, this is because the third party is funded by the very companies it is meant to oversee and therefore lacks any real independence.

Self-regulation has been less than successful at protecting privacy and for the most part has lead to a "race to the bottom" effect within the marketplace. In the absence of direct requirements to abide by proper privacy standards, the industry has been slow to respond to the demands of consumers claiming that their current business models and indeed the whole future of e-commerce depends on the ability to collect and disseminate personal information. Although the Federal Trade Commission (FTC) has been operating as the "de facto" privacy agency, in truth it lacks the basic powers of oversight and enforcement and has not been effective in protecting the privacy of individuals.

The FTC has held many workshops on privacy, published educational material for consumers, and made statements concerning the privacy principles that companies should abide by and disclose in their privacy policies. In general it tries to encourage businesses to comply with "Fair Information Practices;" however, it has no power to require them to do so. Moreover, it defines Fair Information Practices as only including the rights of notice, choice, access and security instead of the broader class of rights set out in the HEW Report, the OECD guidelines or the Council of Europe Convention. Notably absent from this definition is any sort of "collection limitation" principle prohibiting the collection of excessive data or its storage for a time longer than necessary. In addition, requiring data collectors to give users a "choice" over the collection of their personal information implies a much lower level of protection for individuals than requiring collectors to obtain actual "consent."[67]

When companies do commit to posting good privacy policies the FTC has a limited oversight and enforcement role. Under section 5 of the Federal Trade Commission Act, it may take actions against companies for "unfair and deceptive practices." This provision has been very narrowly interpreted as including only a violation of a former

63 Public Law 95-630
64 Public Law 106-102
65 The *Standards for Privacy of Individually Identifiable Health Information; Final Rule* was issued by the Department of Health and Human Services (DHHS) on December 28, 2000 pursuant to the Health Insurance Portability and Accountability Act 1996 (Public Law 104-191). The rules became effective on April 14, 2001
66 The 1973 HEW Report addressed the shortcomings of this sectoral approach. Speaking in the context of laws on the public sector prior to the passing of the 1974 Act they say " Although there is a substantial number of statutes and regulations that collectively might be called the "law of personal data record keeping," they do not add up to a comprehensive and consistent body of law. They reflect no coherent or conceptually unified approach to balancing the interests of society and organizations that compile and use records against the interests of individuals who are the subjects of records." HEW Report, supra n.28 at 34-5.
67 Rotenberg, supra n.21, at para 30

written agreement (such as a privacy policy). This leads to an anomalous situation within the law whereby a company without a privacy policy is arguably less likely to be punished for privacy invasive practices than a company with a privacy policy. In its own words:

> "[T]he Commission lacks authority to require firms to adopt information practice policies or to abide by the fair information practices principles on their web sites."[68]

Finally, individuals have no right to private action under the FTC Act nor can they compel agency action on their behalf. Consumers are entitled to refer privacy complaints to the FTC but it is not under any obligation to review or even respond to individual cases.[69] Where the agency does take a case, it acts entirely according to its own discretion. There is no opportunity for individuals to be involved and even judicial review is expressly precluded by the Act.[70]

The FTC has submitted three reports to Congress analyzing the effectiveness of self-regulation. The first was in 1998 and found that although 92% of the 1,400 websites surveyed gathered personal information, a mere 14% provided any form of notice to consumers with less than 2% having clearly displayed privacy policies.[71] The 1999 report revealed similarly poor results. Although an improvement in the number of websites disclosing privacy policies was found, the vast majority of them (90%) still failed to implement the other fair information practices.[72] The 2000 results showed that most websites now posted privacy policies but that they still failed to implement the other privacy principles.[73] It was found that a mere 20% of sites collecting information implemented in full or in part all four elements of fair information practices.[74]

III. TRADE CONFLICT

As electronic data is so easily transferred across digital networks, an important aspect of most data protection laws is "export restrictions." These prohibit the transfer of information to third-party countries that do not have adequate protections for privacy. In the global marketplace any restriction on the free flow of information would obviously have a most detrimental result on electronic commerce.

The best-known example of such a provision is contained in Article 25 of the EU Data Protection Directive. As this Directive is directly binding on all European Union member states,[75] the inclusion of this trade restriction has had a profound impact on the rest

68 A Federal Trade Commission Report to Congress (May 2000), p34. Available at <http://www.ftc.gov/os/2000/05/index.htm#22>.

69 Code of Federal Regulations Title 16,Chap 1, Part 1, Sec 2.2 empowers "Any individual, partnership, corporation, association, or organization [to] request the Commission to institute an investigation in respect to any matter over which the Commission has jurisdiction." The Commission, however, retains full discretion to decide whether or not to take the action.

70 15 U.S.C.Section 57b-3(c)

71 Federal Trade Commission, *Privacy Online: A Report to Congress*, June 1998, <http://www.ftc.gov/reports/privacy3/toc.htm >.

72 Federal Trade Commission, *'Self-Regulation and Privacy Online: A Report to Congress'*, July 1999, http://www.ftc.gov/os/1999/9907/privacy99.pdf

73 Federal Trade Commission, '*Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*', May 2000, http://www.ftc.gov/os/2000/05/index.htm#22.

74 Three similar studies have been conducted by the Electronic Privacy Information Center (EPIC) in the last number of years. The first, conducted in 1997, reviewed the top 100 most frequently visited web sites on the Internet. Looking for compliance with the original principles of Fair Information Practices, it checked whether sites collected personal information, had established privacy policies, made use of cookies, and allowed people to visit without disclosing their actual identity. Results showed that only 17 of the 100 sample websites had explicit privacy policies and that none met basic standards for privacy protection. (*Surfer Beware: Personal Privacy and the Internet*, June 1997, <http://www.epic.org/reports/surfer-beware.html>.) The second report, in 1998, surveyed the privacy policies of 76 new members of the Direct Marketing Association (DMA) to see whether they conformed with an October 1997 DMA policy announcement requiring all future members to post a privacy policy and provide an opt-out capability. (*Surfer Beware II: Notice Is Not Enough*, June 1998, <http://www.epic.org/reports/surfer-beware2.html>.) Of the 76 new members examined, only 40 had Web sites. Of these, only eight sites had any form of privacy policy, and only three had privacy policies that satisfied the DMA's requirements. None of the sites examined allowed individuals to gain access to their own information. The third report reviewed the privacy practices of the 100 most popular e-commerce websites on the Internet. The report looked for compliance with "Fair Information Practices" or basic data protection guidelines. It also examined whether the sites utilized profile-based advertising and employed cookies in their website operations. Results showed that although most sites displayed a privacy policy, not one of them adequately addressed all the elements of Fair Information Practices. The report also found the privacy policies at many websites to be confusing, incomplete, and inconsistent. 35 of the sites had profile-based advertisers operating on their pages, and 86 of the e-commerce operations used cookies. (*Surfer Beware III: Privacy Policies without Privacy Protection*, December 1999, <http://www.epic.org/reports/surfer-beware3.html>.)

75 Under European Community law rules member states are required to implement Directives into national law within a certain period of their introduction. Under the present directive, the due date for implementation was October 1998. Not all European member states have yet met this obligation. The European Commission is currently pursuing action against those states that are still in default. See Press Release, 11 January 2000 <http://europa.eu.int/comm/internal_market/en/media/dataprot/news/2k-10.htm>.

of the world. Realizing that they could be cut off from dealing with all 15 member states of the European Union, most countries have been moving towards an approach for privacy protection that is more consistent with the European model. For example, Canada and Australia have recently introduced new comprehensive data protection laws.[76] In Latin America more and more countries are introducing the right of *habeas data* which is enforceable against any data collector whether public or private.[77] Chile, Argentina and Paraguay have also recently introduced data protection laws.[78] In addition, many countries in Central and Eastern Europe, such as the Slovak Republic, Latvia, Lithuania, the Czech Republic, and Hungary have adopted new laws based on the European Union Data Protection Directive in part to advance their accession to the European Union but also to prevent any data flow restrictions in the interim.[79]

The U.S., however, has decided to take more of a *sui generis* approach. Although it was never formally ruled upon, there were serious doubts whether the United States' sectoral and self-regulatory approach to privacy protection would pass the adequacy test laid down by the Directive. The EU commissioned two prominent U.S. law professors, who wrote a detailed report on the state of U.S. privacy protections and pointed out the many deficiencies in U.S. targeted approach to data protection.[80]

In 1998, the U.S. began negotiations with the EU to develop an agreement known as "Safe Harbor" to ensure the continued transborder flows of personal data. The idea of the "Safe Harbor" was that U.S. companies would voluntarily self-certify to adhere to a set of privacy principles worked out by the U.S. Department of Commerce and the Internal Market Directorate of the European Commission. These companies would then have a presumption of adequacy and they could continue to receive personal data from the European Union. Negotiations were long and drawn out and subject to bitter criticism by privacy advocates and consumer groups on the one hand, who argued that the agreement would fail to provide European citizens with adequate protection for their personal data, and business lobbyists on the other hand, who argued that the agreement was over-burdensome and would impose significant costs on U.S. businesses. On July 26, 2000, the Commission finally approved the agreement with a promise to re-open negotiations on the arrangement if the remedies available to European citizens prove inadequate.[81]

The future of U.S.-EU data flows, however, is far from settled. So far only thirty-eight companies have signed up to the Safe Harbor agreement[82] and early indications from the new Bush administration signal a strong resistance to other means of ensuring privacy protection for cross-border data flows. On March 23, 2001 representatives from the Departments of Commerce and Treasury sent a letter to the European Commission Internal Market Directorate criticizing model contractual clauses proposed by the Commission to be used in the exchange of consumer information between EU and U.S. companies not covered by the "Safe Harbor."[83] The letter states that the requirements are "unduly burdensome" and "incompatible with real world operations" and warned that "there is a serious danger the adoption of the standard clauses as drafted will create a *de facto* standard that would raise the

76 Supra, n.54
77 Supra n.12
78 See, Privacy International, *The International Privacy Newswire*, <http://www.privacyinternational.org/parts/index.html>
79 As we have seen, Canada and Australia have recently introduced new comprehensive data protection laws. In Latin America more and more countries are introducing the *habeas data* right. This right is enforceable against any data collector whether public or private. In 1999 Chile became the first Latin American country to introduce a data protection law. Banisar, supra n.4 at 86. Argentina and Paraguay have since followed suit. (See, Privacy International, *The International Privacy Newswire*, <http://www.privacyinternational.org/parts/index.html>) In addition, many countries in Central and Eastern Europe, such as the Slovak Republic, Latvia, Lithuania, the Czech Republic, and Hungary have adopted new laws based on the European Union Data Protection Directive and containing similar provisions in part to advance their accession to the European Union and also to prevent any data flow restrictions in the interim.
80 Paul M. Schwartz and Joel R. Reindenberg, *Data Privacy Law*, (Michie) (1996).
81 Commission Decision on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the U.S. Department of Commerce. <http://europa.eu.int/comm/internal_market/en/media/dataprot/news/decision.pdf>.
82 *See*, Safe Harbor List, (http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list). Visited April 18, 2001.
83 As the Safe Harbor only applies to companies overseen by the U.S. Federal Trade Commission and the U.S. Department of Transportation, companies such as those in the financial and telecommunications sectors are automatically excluded.

bar for U.S firms."[84] It urged the European Commission to defer any further consideration of the standard model contracts for data transfers. The European Commission, however, does not seem likely to cede on this point. In response to this letter a spokesman for the Commission said that the U.S. position "appears to be based on a total, complete and utter absence of understanding of what the Commission is doing."[85] Further negotiations are therefore to be expected with suggestions that the issue may eventually end up before the World Trade Organization.[86]

CONCLUSION

Considering that so much of the early legal protections for privacy developed within the U.S., it is somewhat puzzling that it now lags so far behind in the protection of individuals' personal information. Professor Stefano Rodota, Chairman of the EU Data Protection Working Party, calls it an "amazing paradox" that while "[p]rivacy was 'invented' in the U.S., and has long been considered to be typical of American society… Europe is nowadays the region of the world where personal data is most protected." [87]

We have seen the kind of problems this divergence is causing on the international front. On the national front, it is damaging trust and confidence in the electronic marketplace[88] and has become a number one social concern for the 21st century.[89] Unless the situation is quickly addressed it will likely lead to a growing resentment among the U.S. population that their data is less protected than in most other countries around the world, including former dictatorships and communist countries.

When self-regulation was first proposed, it was promised that the policy would be revised if it did not prove effective at protecting privacy.[90] It is now clear that self-regulation has not, and can not, effectively protect privacy in the Information age. In order to avoid unnecessary trade conflicts and to ensure freedom and privacy for U.S. citizens, it is time to carry out this "revision" and to establish baseline principles for privacy within the law.

---

84 The draft version of the European Commission's Model Contract Provisions and comments of the U.S. Department of Commerce (including the March 23 letter) are available at http://www.export.gov/safeharbor/Model_Contract.htm

85 *International Economy: EU-U.S. clash over personal data: private right or commercial opportunity?* , by Peronet Despeignes and Deborah Hargreaves, *Financial Times*, March 29, 2001 available at <http://globalarchive.ft.com/globalarchive/articles.html?id=010329000406>.

86 Although, the Agreement Establishing the World Trade Organization Annex 1B: General Agreement on Trade in Services, Annex on Telecommunications, Art. XIV c(ii) does contain an exemption for measures relating to the "protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts for privacy protections" arguments that Art 25(6) of the EU Directive may constitute a barrier to free trade are still made. Rep. Billy Tauzin, Chairman of U.S. House of Representatives Committee on Energy and Commerce Committee, holding a hearing on March 8, 2001, on the "EU Data Protection Directive: Implications for the U.S. Privacy Debate" (http://www.house.gov/commerce/hearings/03082001-49/08082001.htm) is quoted as having said that "[t]he EU privacy directive….could be the imposition of one of the largest free trade barriers ever seen." Patrick Ross, "Congress fears European privacy standards," CNET News.com, March 8, 2001 (http://news.cnet.com/news/0-1005-200-5070401.html). Also, Peter Swire & Robert Litan in, None Of Your Business: World Data Flows, Electronic Commerce, And The European Privacy Directive 145, 189 (1998) cited in Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 Yale J. Int'l L. 1, (2000) at n.193 suggest that article 25 constitutes an attempt to level the playing field in favor of EU businesses by imposing the same restrictions that they are subject to on U.S. companies. They also suggest that it may unfairly discriminate against U.S. businesses by encouraging firms in Europe to do more business with other European based firms to whom they can freely transfer data rather than to U.S. firms. Shaffer discredits this argument, however, stating that any case brought before the WTO by the U.S. would likely fail on at least three grounds: 1. The EU Directive applies equally to all nations and is therefore not discriminatory on its face; 2. The EU has a legitimate public policy ground for imposing this requirement and this is explicitly recognized in article XIV of GATS (see above) 3. The WTO would be slow to intervene in a case that concerned the balancing of trade with privacy interests. Furthermore he notes that any restriction on trade would likely hurt EU companies as much as U.S. companies in light of the central role of the U.S. in electronic commerce activities. Id. at 50-52.

87 Professor Stefano Rodota Chairman, testimony his testimony before the Subcommittee on Commerce, Trade, and Consumer Protection, id., available at http://energycommerce.house.gov/107/hearings/03082001Hearing49/Rodota100.htm."

88 A recent study by Forrester Research found that privacy concerns accounted for $2.8 billion in lost sales in 1999. See, *The Privacy Best Practice*, Forrester Research, September 1999 at 2.

89 Wall Street Journal/NBC News poll, 1999. This survey also found that "Americans show greater concern for privacy than overpopulation, terrorist acts, racial tensions, and global warming."

90 In a 1997 White House release, former President Clinton and Vice President Gore stated that " [t]he Administration considers data protection critically important. We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy." See, *A Framework for Global Electronic Commerce*,, July 1, 1997 <http://www.ecommerce.gov/framewrk.htm>.