Data Protection and Privacy in the United States and Europe

by Jean Slemmons Stratford & Juri Stratford *

Introduction

The rapid expansion in electronic communications and commerce over the past several years has raised concerns in the United States over personal privacy in an online environment. These concerns have captured the attention of the public, the media, and policy-makers, and there is new interest in the United States in explicit policies protecting the privacy of electronic transactions and personal information. These efforts continue a pattern of policies directed at subject-specific information, such as the *National Education Statistics Act of 1994* that tightened access to personal data collected in the field of education [1].

This pattern is a sharp contrast to the privacy and data protection polices in Europe. Where the U.S. approach has been to provide specific and narrowly applicable legislation, in Europe there are unified supra-national policies for the region. Most countries have implemented these policies with omnibus legislation. The European legislation outlines a set of rights and principle for the treatment of personal data, without regard to whether the data is held in the public or private sector. In the United States, the legal tradition is much more concerned with regulating data collected by the federal government. This paper will review and contrast the development of data protection policies in the United States and Europe.

What Is Privacy?

Privacy is an important, but illusive concept in law. The right to privacy is acknowledged in several broad-based international agreements. Article 12 of the *Universal Declaration of Human Rights* and Article 17 of the *United Nations International Covenant on Civil and Political Rights* both state that, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." The international concept of "the right to privacy" traces its roots to the U.S. Constitution and to common law [2].

A hallmark article in the *Harvard Law Review* in 1890 is widely credited as establishing the right to privacy as a tradition of common law [3]. In that article, Samuel Warren and Louis Brandeis defined that right as "the right to be let alone" [4]. They argued that the right to privacy that afforded to intellectual and artistic property in common law is founded, not on principle of protection of private property, but on that of "inviolate personality" [5].

The term "privacy" does not appear in the U.S. Constitution or the Bill of Rights. However, the U.S. Supreme Court has ruled in favor of various privacy interests-deriving the right to privacy from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments to the Constitution. In 1977 in *Whalen v. Roe*, the Supreme Court first recognized the right to information privacy [6]. It noted that the Constitution protected two kinds of individual interests: "One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions" [7]. Several other decisions have balanced the right to privacy against other compelling interests. The Supreme Court upheld a New York law that required the state to maintain computerized records of prescriptions for certain drugs because the program did not pose "a sufficiently grievous threat" [8]. In *Nixon v. Administrators of General Services*, the Court upheld the federal statute that required national archivists to examine written and recorded information accumulated by the president [9]. The Court ruled that while "the appellant has a legitimate expectation of privacy in his personal communications," that right must be weighed against the important public interest in preservation of materials [10]. The Court did not believe that the appellant's privacy interest was a match for the competing public interest [11].

U.S. Data Protection Laws

There is no single law in the United States that provides a comprehensive treatment of data protection or privacy issues. In addition to the constitutional interpretations provided by the courts and the international agreements mentioned above, there have been a number of laws and executive orders dealing specifically with the concept of data protection. The most important and broad based of these laws are *the Privacy Act of 1974* and the *Computer Matching and Privacy Act*. These laws deal exclusively with personal information held by the federal government

and do not have any authority over the collection and use of personal information held by other private and public sector entities.

The *Privacy Act* (PL 93-579) is a companion to and extension of *the Freedom of Information Act (FOIA)* of 1966. *FOIA* was primarily intended to provide access to government information. It did exempt the disclosure of personnel and medical files that would constitute "a clearly unwarranted invasion of personal privacy" [12]. This provision was initially used to deny access to people requesting their own records. So the *Privacy Act* was also adopted both to protect personal information in federal databases and to provide individuals with certain rights over information contained in those databases. The act has been characterized as "the centerpiece of U.S. privacy law affecting government record-keeping" [13]. The act was developed explicitly to address the problems posed by electronic technologies and personal records systems and covers the vast majority of personal records systems maintained by the federal government. The act set forth some basic principles of "fair information practice," and provided individuals with the right of access to information about themselves and the right to challenge the contents of records. It requires that personal information may only be disclosed with the individual's consent or for purposes announced in advance. The act also requires federal agencies to publish an annual list of systems maintained by the agency that contain personal information.

The law had originally proposed the creation of a privacy protection commission; however, then President Gerald Ford was opposed to such a bureaucracy. He wrote

> I do not favor establishing a separate Commission or Board bureaucracy empowered to define privacy in its own terms and to second-guess citizens and agencies. I vastly prefer an approach which makes Federal agencies fully and publicly accountable for legally-mandated privacy protections and which gives the individual adequate legal remedies to enforce what he deems to be his own best privacy interests [14].

As a compromise, central oversight was assigned to the Office of Management and Budget, and OMB has exercised relatively weak leadership in the implementation of the *Privacy Act*. The law also calls for the designation of Privacy Act officers within federal executive agencies to handle requests and insure compliance with the code of practice. Ultimately enforcement rests with the courts (as individuals bring suit to redress perceived grievances).

Under the umbrella of the *Privacy Act*, Congress has also enacted *the Computer Matching and Privacy Protection Act of 1988* (PL 100-503). This act amended the *Privacy Act* by adding new provisions regulating the use of computer matching. Computer matching is the computerized comparison of information about an individual for the purpose of determining eligibility for Federal benefit programs, or for the purpose of recouping payments or delinquent debts under such programs.

In general, matching programs involving Federal records must be conducted under an agreement between the source and recipient agencies. This agreement describes the purpose and procedures for the matching and establishes protections for the matched records. The agreement is subject to review by a Data Integrity Board and each agency involved in matching activities must establish such a board. While the law provides no special access rights to individuals; agencies must notify individuals of any findings based upon a computer matching program before taking any adverse actions; and individuals must be given the opportunity to contest such findings.

The *Computer Security Act of 1987* (PL 100-235) also deals with personal information in federal record systems. It protects the security of sensitive personal information in federal computer systems. The act establishes government-wide standards for computer security and assigns responsibility for those standards to the National Institute of Standards. The law also requires federal agencies to identify systems containing sensitive personal information and to develop security plans for those systems.

Narrowly Applicable Laws

There are also numerous narrowly applicable laws on privacy and data protection. These laws generally fall into two distinct categories. The first governs the status of information held by the federal government. In general, these laws provide declarations regarding the confidentiality of specific types of personal information, provide guidelines for their disclosure and penalties for infringement of the individual's right to privacy.

As examples, 13 *U.S.C.* 9 absolutely prohibits any use of personally identifiable data from the Census except by sworn officers and employees of the Census Bureau. Similarly 42 *U.S.C.* 242m protects against the disclosure of personal information gathered by the National Centers for Health Services Research and for Health Statistics for research purposes. The *National Education Statistics Act* (PL 103-382) re-authorized and amended provisions for the National Center for Educational Statistics and the National Assessment of Educational Progress. The act dramatically revised the confidentiality and dissemination practices of the center. The *Tax Reform Act (*PL 94-455) makes tax returns and return information confidential, permits only limited disclosure of returns and returns information for specific purposes, and specifies procedures for disclosure. The law also authorizes persons whose tax returns or return information is disclosed in violation of this Act to bring a civil action for damages and costs of the action, and establishes criminal penalties for wrongful disclosures.

The United States has largely avoided legislation governing the treatment of sensitive personal information in records systems held by sources other than the federal government. The few laws that deal with these systems tend to address the treatment of personal financial information. For example, *The Fair Credit Reporting Act* (90-321) regulates the use of individual personal and financial information by consumer credit reporting agencies. It assures that information is accurate and complete, relevant to the purpose for which it is used, and upholds the individual's right to privacy.

A limited number of laws have been passed to deal with issues outside the financial arena. These laws have generally been implemented in response to specific perceived abuses. As an example, the *Video Privacy Protection Act of 1988* (PL 100-618) amends the Federal criminal code to prohibit, with certain exceptions, the disclosure of video rental records containing personally identifiable information. It permits any person who is aggrieved by a violation of this Act to bring a civil action for damages; and requires the destruction of personally identifiable records within a specified period of time. This law was passed in the wake of criticism following the release and publication of Robert Bork's video rental records, during his consideration as a nominee to the Supreme Court [15].

Several U.S. laws do restrict the federal government's access to records held by other sources. Until the rise of the Internet, misuse of personal data held by entities other than the federal government did not command much attention from policymakers as a threat to privacy or personal liberty. However, government access to these records did seem to be a cause for concern as several laws have restricted federal access to information held in such systems. Typically, agencies must obtain permission or a court order to get access to these records [16]

Data Protection in Europe

There are two important supra-national policies in Europe in relation to data protection. The first is the Council of Europe's *Convention on Data Protection*, and the second is the EU *Data Directive*. In contrast to U.S. privacy law, privacy protection in Europe is addressed by omnibus legislation covering both public and private sectors

The Council of Europe was set up after the Second World War to help unite Europe by

> fostering closer relations between the states belonging to the community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe … and promoting democracy on the basis of the fundamental rights recognized in the constitutions and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms [17].

That *Convention* recognizes the right to privacy as one of the fundamental human rights. The Council's concern with the processing of personal information grew slowly with advances in information technology and the increase in the use of such data. In the late 1960s, the Council's Committee of Experts on Human Rights conducted a survey with regard to human rights and modern scientific and technological developments. It concluded that existing laws did not provide adequate protection for individuals given the developments in these areas. Several other committees examined various aspects of the problem and came to similar conclusions. In 1976, the Council established a Committee of Experts on Data Protection that reported its findings in early 1979 and the result was the Council of Europe's *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. The Council of Europe *Convention* sets forth the data subject's right to privacy, enumerates a series of basic principals for data, provides for transborder data flows, and calls for mutual assistance between parties to the treaty including the establishment of a consultative committee and a procedure for future amendments to the convention [18].

The Commission of the European Community recommended that member states ratify the Council of Europe *Convention* and warned that it might introduce its own directive on the subject. When it did so, the primary purpose of the directive was to further standardize the level of protection across the Community. The EU *Data Protection Directive* reaffirms the principals outlined in the Council of Europe *Convention* [19].

Major components of the Directive acknowledge the individual's right to privacy. The Directive sets standards for the treatment of personal data collected from individuals and for individuals rights of access, notification, and correction. Of particular interest to the United States is the Directive's treatment of data transfers to countries outside the EU. Article 25 governs the "Transfer of Personal Data to Third Countries." EU Member States may transfer personal data only after determining that "the third country in question ensures an adequate level of [data] protection." The EU shall consider the "rules of law…in the third country" to make this determination.

The Directive was adopted in October 1995, and called for member states to bring their national privacy laws into compliance within three years. These national laws are now going into force across Europe.

The absence of generic privacy legislation in the U.S. is a major concern to the EU nations and this will make determination that the U.S. ensures an adequate level of

protection unlikely. While there are concerted efforts in the administration calling for privacy legislation covering various types of data (e.g. Secretary of Health and Human Services Shalala made recommendations to Congress on the Confidentiality of Individually-Identifiable Health Information on September 11, 1997,) the large number of bills in Congress dealing with privacy issues suggests that the U.S. may continue to take a piece-meal approach to privacy legislation [20].

However, the EU is unlikely to issue an across-the-board finding that U.S. privacy protections are inadequate. The EU could demonstrate its seriousness about the Directive by initially singling out one or more U.S. companies or sectors as not meeting the adequacy test; e.g. any company handling personal medical information [21].

Given policy traditions in the U.S., it is likely that data protection in the private sector will be largely self-regulatory. The Federal Trade Commission has been working with the private sector to develop voluntary codes of conduct, but it is unclear where these efforts will lead. It is difficult to say whether the EU will be able to recognize such an approach as adequate. If the EU decides that the largely self-regulatory approach followed by the U.S. is not sufficient to justify an adequacy finding, a much broader embargo is possible [22]. Privacy and data protection are likely to continue to be big issues in U.S. domestic and international policy. It will be interesting to see how these issues will resolve themselves, or if there is to be a major clash between the U.S. and Europe.

Footnotes

[1] *U.S. National Education Statistics Act of 1994.* P.L. 103-382 *U.S.C.*, 9001-9012.

[2] United Nations, General Assembly, 3rd Session. "Resolution 217A Universal Declaration of Human Rights," 1948. *The International Covenant on Civil and Political Rights* was adopted by the General Assembly of the United Nations in *Resolution 2200 (XXI)* of 16 December 1966. For the full text of the Resolution and the Covenant, see *Official Records of the General Assembly,* Twenty-first Session, Supplement No. 16 (A/6316), 49.

[3] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4 (1890):193-220.

[4] Warren and Brandeis, 193.

[5] Warren and Brandeis, 205.

[6] *Whalen v. Roe,* 429 *U.S. Reports* (February 22, 1977), 589-604.

[7] *Whalen v. Roe,* 599-600.

[8] *Whalen v. Roe,* 600.

[9] *Nixon v. Administrators of General Services,* 433 *U.S. Reports* (28 June 1977), 425-484.

[10] *Nixon v. Administrators of General Services,* 465.

[11] *Nixon v. Administrators of General Services,* 465.

[12] *Freedom of Information,* Title 5 *U.S.C.* 552(b) (6).

[13] Robert Aldrich, "Privacy Protection Law in the United States," (NTIA Report 82-98) in U.S. Congress. House. Committee on Government Operations. *Oversight of the Privacy Act of 1974: Hearings.* 98th Congress, 1st Session, 7-8 June 1983, 489 (Y4.G74/7:P93/11/974).

[14] U.S. Congress. House. Committee on House Administration. *Legislative History of the Privacy Act of 1974, S.3418 (Public Law 93-579): Source Book on Privacy.* 94th Congress, 2nd Session, 1976, Joint Committee Print (Y4.G74/6:L52/3).

[15] Priscilla Regan, *Legislating Privacy: Technology, Social Values and Public Policy.* (Chapel Hill: University of North Carolina Press, 1995), 199.

[16] Aldrich, "Privacy Protection," 505-507.

[17] Commission of the European Community. *Communications on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security,* Com (90)314.SYN 287, 44.

[18] Sarah Ellis and Charles Oppenheim. "Legal Issues for Information Professionals, Part III: Data protection and the Media – Background to the Data Protection Act 1984 and the EC Draft Directive on Data Protection," *Journal of Information Science* 19 (1993):85.

[19] "Directive 95/46/EC of the European Parliament and of the Council of 24 October on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data," *Official Journal of the European Community* 23 November 1995, no.L281, 31.

[20] Rebecca Vesely. "Cop-friendly Approach to Handling Medical Data," *Wired News* 12 (September 1997) (URL http://www.wired.com/news/news/politics/story/6824.html)

[21] Peter B. Swire and Robert E. Litan, Avoiding a Showdown over EU Privacy Laws, Brookings Policy Brief, no. 29 (February 1998) (URL http://www.brook.edu/comm/policybriefs/pb029/pb29.htm)

[22] *Ibid*.

* Paper presented at the IASSIST Conference, May 21, 1998, at Yale University, New Haven, Connecticut. Jean Slemmons Stratford, University of California, Davis, and Juri Stratford, University of California, Davis.