January 1996

Filling the Void of Data Protection in the United States: Following the European Example

Michael P. Roch

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Recommended Citation
Available at: http://digitalcommons.law.scu.edu/chtlj/vol12/iss1/3
FILLING THE VOID OF DATA PROTECTION IN THE UNITED STATES: FOLLOWING THE EUROPEAN EXAMPLE*

Michael P. Roch†

Table of Contents

I. INTRODUCTION ........................................ 72

II. HISTORY OF DATA PROTECTION IN EUROPE .......... 72
   A. World-wide Data Protection: the OECD Guidelines .. 73
   B. Early European Data Protection Efforts: the European Convention .......................... 75
   C. Precursor to the European Draft Directive: National Efforts ............................ 76

III. THE EUROPEAN DRAFT DIRECTIVES ON DATA PROTECTION ........................................ 79
   A. The 1992 Amended Proposal on Data Protection .... 80
      1. Objectives and General Provisions ............. 80
      2. Data Quality ................................... 82
      3. Conditions on the Processing of Personal Data ... 83
      4. The “Data Subject’s Bill of Rights” ............. 83
      5. Transborder Data Flows ........................ 85
   B. The 1994 Network Draft ............................ 86

IV. DATA PROTECTION IN THE UNITED STATES .............. 88
   A. The United States Constitution and the Supreme Court ........................................ 88
   B. Acts of Congress ................................... 89
   C. Common Law ...................................... 92

V. FILLING THE VOID OF DATA PROTECTION IN THE UNITED STATES: FOLLOWING THE EUROPEAN EXAMPLE .... 93

VI. OBSERVATIONS AND CONCLUSIONS ...................... 95

* Copyright © 1995 Michael P. Roch
† Michael P. Roch, C.P.A.; Candidate, J.D., University of Denver College of Law, 1996; Master of Accountancy, University of Denver School of Accountancy, 1991. Mr. Roch served as a management consultant in Central Europe prior to attending law school in the United States; among other projects he participated in the planning of the privatization of Slovenia’s Telecom.

71
I. INTRODUCTION

Governmental record keeping of individual data is as old as civilization itself. The industrial revolution of the nineteenth century and the technological revolution since the mid-1960s have made the record keeping of such data much easier and more comprehensive. In the past two decades, computer science has advanced at an abnormally high rate of speed. As the cost of computing power and storage capacity drops, businesses increasingly use computer technology for record keeping, market analysis, and managerial decision making; governmental agencies increasingly use computer technology for keeping census data, for tracking program participants, and for intelligence purposes. As a result, data about citizens are gathered and kept in at least one commercial or governmental data base. Questions that soon arise are: "Who keeps data about me? What is being stored? Why? Who has access to my personal data? How will those data harm me?" All of these questions raise one common concern, namely, whether an individual's privacy with regard to an individual's data is adequately protected.

Many European nations have passed data protection laws as part of national privacy legislation to address this concern. Those data protection laws address the right to have some control over the collection, storage, use, and dissemination of one's personal data. In order to have consistent laws throughout Europe, the European Commission will soon pass several directives. In the United States, however, virtually no such laws exist — putting private, personal information of American citizens at risk of public disclosure and scrutiny.

This article first addresses the origins of data protection both globally and in Europe, focusing on the most recent directives under consideration by the European Commission. This article then briefly summarizes the few existing data protection statutes in the United States and concludes with recommendations as to how the United States could remedy some of the shortcomings in this area of law.

II. HISTORY OF DATA PROTECTION IN EUROPE

The history of data protection is rooted in the efforts of European nations, particularly the Federal Republic of Germany, to curb the

2. Data protection is technically a type of privacy concern. Privacy includes an individual's right to be free from brazen police searches and from wiretapping; privacy also includes the right to make private decisions within one's family. See id. at 13.
3. Id.
threat of improper use of personal data. These nations' concerns are also manifested in global and regional efforts. The two organizations that have contributed early on to the harmonization of data protection regulation are the Organization for Economic Cooperation and Development (OECD)\(^4\) and the Council of Europe.\(^5\) Their efforts are considered the forefathers of the Amended Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data,\(^6\) as currently under discussion by the European Council.\(^7\)

To show the history behind the individual provisions of the Amended Proposal, this section summarizes the efforts of the OECD and the Council of Europe. This section then provides a brief view of how various European nations, especially the Federal Republic of Germany,\(^8\) have dealt with national data protection issues.

### A. World-wide Data Protection: the OECD Guidelines

Concurrent with the development of data protection laws in individual countries and in the Council of Europe, the OECD studied the need for uniform data protection laws.\(^9\) In 1980, after two years of investigation,\(^10\) the OECD established broad, voluntary guidelines for the protection of personal data.\(^11\) These guidelines significantly parallel the recommendation of the European Convention.\(^12\)

---


5. See infra part II.B. The Council of Europe is not the equivalent to the European Union. The Council of Europe was founded in 1948 by several European nations in order to further unities among its members and to promote civil liberties. Hillary E. Pearson, Data Protection in Europe, 8 COMPUTER L. 20, 24 fn.1 (1991). See generally A.H. Robertson, THE COUNCIL OF EUROPE (2nd ed. 1961).


7. See Peter Mei, The EC Proposed Data Protection Law, 25 LAW & POL'Y INT'L Bus. 305, 305 (1993). See also infra part III.

8. See infra notes 44-58 and accompanying text.

9. Mei, supra note 7, at 305.

10. Id.


The OECD established as limitations on the collection of personal data that such data should be collected lawfully with the knowledge and consent of the data subject.\(^1\) Data that are collected are to be of certain quality in that they should be accurate, complete, and up to date.\(^2\) The purpose of the data collection effort should be specified.\(^3\) However, the guidelines are unclear as to whom this disclosure should be made. Once such a specification has been made, the collected data may not be used for a different purpose without the data subject’s consent or authority of law.\(^4\) The data gatherer has the burden of protecting stored data from unauthorized access, destruction, use, modification, or dissemination.\(^5\) While the OECD Guidelines represent a first effort to harmonize protection of personal data on a global basis, these principles are written in a very broad manner.

The OECD Guidelines provide that a data subject has the right to inquire what types of data an entity has gathered about the individual.\(^6\) The entity must provide the individual with such information within a reasonable time of the inquiry at a reasonable charge and in a form that is intelligible to the individual.\(^7\) If such information is incorrect, the individual has the right to have such incorrect data erased or corrected.\(^8\)

The OECD Guidelines also provide that the free flow of information across national borders should not be restricted unless the recipient nation “does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation.”\(^9\) The OECD guidelines thus expressed an equivalency standard, which means the recipient nation of a transnational data flow must have data protection laws that protect personal privacy to the same extent as the nations from which it receives data.

In addition to the OECD, the Council of Europe generated certain data protection guidelines that helped influence the Amended Proposal. The Council’s standards are discussed next.

\(^{12}\) OECD Guidelines, supra note 11, Annex, ¶ 7. The OECD Guidelines define the data subject as a person about whom data exist. \textit{Id.} ¶ 1 (b).

\(^{13}\) \textit{Id.} ¶ 8.

\(^{14}\) \textit{Id.} ¶ 9.

\(^{15}\) \textit{Id.} ¶ 10.

\(^{16}\) \textit{Id.} ¶ 11.

\(^{17}\) \textit{Id.} ¶ 13(a), (b).

\(^{18}\) \textit{Id.} ¶ 13(b).

\(^{19}\) \textit{Id.} ¶ 13(d).

\(^{20}\) \textit{Id.} ¶ 13(d).

\(^{21}\) \textit{Id.} ¶ 17.
B. Early European Data Protection Efforts: the European Convention

The European initiative for rules of law relating to data protection originated through the collective efforts of individual European nations. In 1968 the Council of Europe began "to study potential courses for data protection legislation." The European Convention stressed the free flow of data and secondarily addressed protection of individuals. After an extensive period of study simultaneous to that of the OECD, the Council of Europe passed a resolution concerning stored personal data in 1974. Accordingly, the resolution states: a) information about an individual's private life should not be disseminated, b) data gatherers should only store relevant information, c) rules should be implemented regarding collection, storage, and dissemination of data, d) individuals should have the right to know what data are stored where and for what reason, e) individuals should have the right to have incorrect information corrected or deleted, and f) only those entities or individuals with a valid purpose should have access to personal data. These preliminary guidelines became the basis for the first binding Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data in 1981. The European Convention covers both the private and public sectors and establishes quality standards which gatherers of personal data must follow in order to protect all individuals with regard to processed data.

The European Convention specifies that data must be: a) obtained and processed fairly and legitimately, b) stored and used for legal purposes, c) adequate, relevant, and not excessive in relation to the purpose for which they are stored, d) accurate and up to date, and e) maintained only as long as required to achieve their purpose. The European Convention prohibits outright the gathering of information relating to race, political opinion, religious and other beliefs, health,
sexual habits, and criminal convictions unless domestic law provides appropriate safeguards against unauthorized use.  

In addition to standards relating to data quality, the European Convention provides individuals with additional rights, following the model of the German Bundesdatenschutzgesetz of 1977. Individuals may: a) inquire to any data gathering entity as to the existence of a personal data file, b) obtain a copy of the data kept in reasonably legible form, c) obtain correction or erasure of false or otherwise improperly kept data, and d) request that personal data be erased if the data gatherer does not provide the individual access to or a copy of his data. In addition, no state may make exceptions to the quality of data standards and the individual rights created under the European Convention with the exception of issues relating to national security and public safety.

Since the European Convention did not include definitions and was not self-executing, individual countries, in their implementing legislation, have provided their own. This deficiency and the inherent differences between each country's implementing legislation have contributed to a lack of harmony between the European nations' laws. This lack of harmony, in turn, has resulted in provisions restricting flow of data across national boundaries if the recipient country did not have adequate data protection guidelines in the mind of the sender's country. This phenomenon was consistent with the European Convention's language with regard to transnational data flows. The only other circumstance under which the European Convention permitted regulation of transborder data flows remained in the case of transfer through an intermediary party with the purpose of circumventing data protection guidelines.

C. Precursor to the European Draft Directive: National Efforts

European nations recognized early on that, while the computer was a superb tool for the promotion of progress in Europe, the use of computers presented a potential threat to individual privacy. In or-
order to minimize this threat from the outset, Sweden and the Federal Republic of Germany were first to establish data protection guidelines beginning in the 1970s.

Sweden passed the first national data protection law in 1973.40 The Swedish Data Bank Statute principally prohibited the gathering of data about persons without governmental authorization.41 Most importantly, the law established a national Data Inspection Board charged with enforcement of the statute.42 The Data Inspection Board further controls the licensing process over data gathering; the Data Inspection Board may further gain access to data bases to ensure that the entity storing personal data is in compliance with the Data Bank Statute.43

As do the Swedes, Germans value privacy. The German tradition of privacy began in the German Civil Code of 1896 in a provision protecting the credit of individuals that requires "a person making an incorrect statement, which was capable of endangering the credit of another, although [he knows] that such statement is incorrect, is obligated to compensate the other for any damages resulting therefrom."44 After World War II, the right to privacy was imbedded in the German constitution,45 and as a result, Germany has a "scheme of integrated privacy and data protection laws at the federal and state levels."46

In initial cases relating to privacy as applied to the maintenance of data, the German Federal Constitutional Court objected to the government's keeping an inventory of private data of individuals by means of confidential government census.47

The German state of Hesse passed the first Data Protection Law in 1970, "but it applied only to the public sector, and was merely a state, not a federal, law."48 The German federal government followed the Hessen model when it passed the Law on the Protection of Personal Data Against Misuse in Data Processing.49

40. Id. at 902-03.  
41. Id. at 902.  
42. Id.  
43. Id. at 902-03.  
44. Böhlhoff and Baumanns, supra note 12, at 175.  
47. Böhlhoff and Baumanns, supra note 12, at 175 (citing Federal Constitutional Court, Dec. of July 16, 1969, BVerfGE 27, 1(6)).  
The German Bundesdatenschutzgesetz of 1977 applied to both the public and the private sectors and covered manual as well as automated processing of personal data of natural, not legal, persons. The Bundesdatenschutzgesetz was, thereby, a front runner of the European Convention to which the Federal Republic was a signatory. The provisions of the Bundesdatenschutzgesetz are essentially similar to those of the European Convention and the OECD Guidelines, except for various additional provisions.

The German Bundesdatenschutzgesetz includes the establishment of supervisory bodies. On the public level, the law requires the establishment of a state supervisory authority charged with the responsibility of assuring compliance; private entities employing five or more persons for data administration purposes have to appoint a “data protection representative” who is charged with the same responsibility as the public state agency. Since this administrator still reports to management, his only true remedy is to report alleged violations to the state authority.

While the OECD Guidelines require that the recipient nation’s data protection standards must afford equivalent protection as under OECD Guidelines, German law is silent as to whether transborder data flows are permissible. It appears, therefore, that they are permissible under most circumstances. This issue of transborder data flows became important during the negotiations of the Treaty of Unification between the Federal Republic of Germany and the German Democratic Republic due to the vast amounts of data collected by the East German state police on the activities and beliefs of individuals. The treaty reiterated that data may only be transmitted for legitimate purposes, and the recipient may not distribute these data for purposes other than those specified by the transmitter. The treaty defers to the European Convention for the parties’ conduct with respect to data protection.

50. Cole, supra note 24, at 904.
51. See supra part II.B.
52. Böhloff and Baumanns, supra note 12, at 177.
53. Id.
54. Id. See also Bennett, supra note 1, at 74-82 (providing an excellent summary of the German data protection laws).
55. Böhloff and Baumanns, supra note 12, at 179.
57. Id. Annex VII ¶¶ 1-4.
III. THE EUROPEAN DRAFT DIRECTIVES ON DATA PROTECTION

Since the data protection guidelines of both the OECD Guidelines and the European Convention are of rather general nature, different standards of data protection among European Union members have developed. In response, the European Commission in 1990 issued three proposals serving to protect personal data rights. The first deals with individuals' rights regarding processing of personal data; the second addresses the protection of personal data with respect to electronic data networks; the third specifically confronts information security. The Economic and Social Committee commented on all three proposals simultaneously in April 1991, reemphasizing that individual privacy must be strictly protected. Considering the proposed changes, the European Commission issued an amended proposal of individuals' rights regarding processing of personal data in 1992. The Amended Proposal did not pass as expected in late 1993 or by the implementation deadline of July 1, 1994; instead, the European Commission issued an amended proposal for the protection of personal data with respect to electronic data networks in June of 1994, designed to supplement the general directive. This section

59. Pearson, supra note 5.
64. Id. art. 1.1.
66. Id. art. 35(1). This delay is partially due to the European Parliament's desire for additional definitions and clarification of the scope of the proposed directive. Commission of the European Communities, Protection of Personal Data: Public Digital Telecommunications Networks, Sept. 12, 1994, at 4.5.11, ¶ 4, available in Lexis, EUROCOM Library, Info-92 File.
summarizes both amended proposals in turn, discussing the strengths and weaknesses of several provisions.

A. The 1992 Amended Proposal on Data Protection

1. Objectives and General Provisions

The Amended Draft, after no less than thirty-four recitals, carefully reiterates in the statement of its objectives the competing interests of data privacy and free flow of personal data between European states; the statement of objectives thereby introduced a conflict which is apparent throughout the Amended Proposal and which required careful balancing on behalf of the Commission.

The Commission determined that the directive should apply to all personal data, whether processed manually or automatically, excluding only the processing of data outside the reach of EC law and processing of personal data by a natural person when done for private purposes. In addition, the Amended Proposal allows member states to implement rules that address how the protection of personal privacy is to balance with the freedom of the press. These scope limitations are significant because they allow the Amended Proposal to address the evil against which remedy is sought: the commercial and governmental use of private data. The fact that the European Commission

stricken to emphasize that, in a change in approach, the directive would apply to private as well as public networks. Id.

68. Network Draft, supra note 67.
69. Amended Proposal, supra note 6, art.1.
70. "Personal data" is defined as:

[A]ny information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity . . . .

Amended Proposal, supra note 6, art. 2(a). Note that this directive only applies to natural, not legal, persons. Entities such as corporations do not enjoy protection under this proposed directive. European Commission, National Implementing Measures; Data Protection; What Can Be Done To Protect Personal Data?, September 8, 1994, available in LEXIS.

71. "Processing" of personal data is defined as:

[A]ny operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Amended Proposal, supra note 6, art. 2 (b). This provision remains subject to debate as several nations oppose the reach of this directive to include manual processing of data. See European Social Policy, No Agreement in Council on Personal Data Protection, Europe Information Service, July 15, 1994, available in LEXIS.

72. Amended Proposal, supra note 6, art. 3.
73. Id. art. 9.
requires businesses as well as governments to ensure that a person’s privacy is not infringed presents one crucial difference between the Amended Proposal and past Congressional efforts, as shall be seen below.

The European Commission charged the individual controller74 of data with the proper implementation75 and enforcement76 of the laws each European state would prescribe following the Amended Proposal’s provisions. This controller is responsible to a supervisory governmental authority charged with the duty of assuring that the country’s provisions comply with those of the Amended Proposal.77 These provisions create a very clear structure. This structure allows governmental agencies to cooperate with businesses to ascertain compliance, and it provides the European citizen with a clear picture of to whom to address violations or abuses of an individual’s rights.

The supervisory body may hear complaints initiated by data subjects.78 Furthermore, the supervisory body has investigative and intervening powers to assure that the processor complies with national laws and the directive; it also is charged with prosecuting violators.79 The nations’ supervisory bodies are also asked to cooperate in order to assure effective enforcement of the directive.80 Multinational corporations, which loathe these provisions because they increase operating costs, should appreciate the efforts of the European Commission to make these, and the corresponding national standards, as uniform as possible. Likewise, the unsuspecting traveller, whether for business or pleasure, is not confronted with inconsistent levels of protection of his personal privacy.

The data controller, in turn, must ascertain that the data are stored in a secured manner, paying due diligence to state of the art technol-

74. A “controller of data” is defined as

[A]ny natural or legal person, public authority, agency, or other body who processes personal data . . . and who decides what [sic] is the purpose and objective of the processing, which personal data are to be processed, which operations are to be performed upon them and which third parties are to have access to them.

Id. art. 2(d).

A “third party” is “any natural or legal person other than the data subject . . . .”

Id. art. 2(f).

75. Id. art. 4.

76. Id. art. 4(2).

77. Id. art. 30(1).

78. Id. art. 30(2).

79. Id. art. 30(2).

80. Id. art. 30(5). The supervisory bodies also elect members to a “working party.” This working party is placed under immediate authority of the Commission and is charged with assuring uniformity of application and enforcement of the directive. See id. arts. 31, art. 32.
ogy;\textsuperscript{81} this applies also to all types of data transfers, including network communications and transmissions over telephone lines\textsuperscript{82} and to data that are processed by an authorized agent of the controller.\textsuperscript{83} The controller must also notify the national supervisory authority and provide very specific information before processing personal data if the controller seeks to gather new types of information or seeks to use presently stored information for a different purpose.\textsuperscript{84}

The function of the data controller is double-edged. On the one hand, the employee of a business charged with this duty must answer to his superiors in his day to day activities; on the other hand, he must assure that the company for which he works both complies with the standards set forth by the Amended Proposal and addresses protection issues raised by individuals. These duties are inherently conflicting. In order to at least partially remedy this conflict, the business should treat this controller as an internal auditor; just as internal auditors report to the Board Audit Committee, the controller of data should report directly to a special committee of the board of directors or of the advisory board.

2. Data Quality

The Amended Proposal sets specific principles relating to data quality, heavily drawing on the quality standards introduced by the European Convention and the OECD Guidelines. While data must be collected for "specified, explicit, and legitimate"\textsuperscript{85} purposes and processed "lawfully and fairly,"\textsuperscript{86} these data must not be excessive or unrelated to the purpose for which they are kept.\textsuperscript{87} Data must also be kept current; old and irrelevant data must be removed.\textsuperscript{88} The basic data quality provisions alone place a substantial burden on the processor of data.\textsuperscript{89} Such rules would, for instance, prevent false or old information to remain present on credit reports; the burden remains on the processor of data, not the data subject, to ascertain that the data are and remain correct. This provision raises the cost of doing business,

\begin{itemize}
\item[81.] The function of the controller is similar under the German Bundesdatenschutzgesetz of 1977. German Bundesdatenschutzgesetz of 1977, supra note 49.
\item[82.] Amended Proposal, supra note 6, art. 17.
\item[83.] Id. art. 24(1) and (2).
\item[84.] See id. art. 18(1)-(3).
\item[85.] Id. art. 6(1)(b).
\item[86.] Id. art. 6(1)(a).
\item[87.] Id. art. 6(1)(c).
\item[88.] Id. art. 6(1)(d).
\item[89.] The processor of data is defined as "any natural or legal person who processes personal data on behalf of the controller." Id. art. 2(e).
\end{itemize}
thereby encouraging processing firms to store only minimal amounts of data to keep liability exposure to a minimum.

3. Conditions on the Processing of Personal Data

Next, the Amended Proposal sets specific conditions under which personal data may be processed. Processing is always allowed with the data subject's consent.\(^9\) If such consent is not given, data may generally be collected if necessary for a legitimate interest, unless that interest is outweighed by the interests of the data subject.\(^91\) This last provision is more restrictive than it appears, because this directive presumes that the individual's right to privacy is paramount.

In addition, these two conflicting interests are not balanced if certain types of data are to be processed. These, again paralleling the European Convention, include data "revealing racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion, or trade union membership, and of data concerning health or sexual life."\(^92\) The data subject must have given written permission for the processing of these data.\(^93\) Religious, political, and similar organizations may, of course, continue to keep a member data base, provided that such data are not disclosed to third parties.\(^94\) In addition, data concerning criminal convictions may only be kept by "judicial and law-enforcement authorities."\(^95\) The Commission singled out these types of data because they represent the very core of an individual's Privatsphäre; most Europeans deeply believe that these special pieces of information are simply no one's business. This is in direct contrast with U.S. citizens who as yet have complained little about their nonexisting rights of data privacy for a variety of cultural reasons that this author has not had the opportunity to explore in depth.

4. The "Data Subject's Bill of Rights"

Following the German Bundesdatenschutzgesetz, the European Commission has granted specific rights to the data subject. First, any person (both natural and legal) has the right to receive detailed infor-
information about a processor of data.\textsuperscript{96} Second, the controller of data must provide the data subject with certain information about the data being sought.\textsuperscript{97} Third, if the data at issue have been lawfully obtained without consent of the data subject, the individual has the right to know to which third parties his data are disclosed,\textsuperscript{98} unless otherwise provided by the Amended Proposal or by a member state’s law.\textsuperscript{99} Fourth, the data subject has the right to access personal data (and their use) kept by a processor or controller of data; such data must be provided in a useable form to the data subject.\textsuperscript{100} Fifth, the data subject has the right to rectify inaccurate or incomplete data.\textsuperscript{101} Sixth, the data subject may compel the controller of data to block or erase data that have been illegally obtained.\textsuperscript{102} Seventh, the processor or controller must cease processing of an individual’s data if the data subject objects to the processing on legitimate grounds.\textsuperscript{103} Eighth, the Amended Proposal provides a private right of action to the data subject for any damages caused by the violation of the directive,\textsuperscript{104} imposing liability on anyone who unlawfully processes personal data.\textsuperscript{105} The controller may raise as an affirmative defense unauthorized access if “he proves that he has taken suitable steps to satisfy the [provisions regarding data security].”\textsuperscript{106} The Amended Proposal leaves imposition of criminal and civil penalties to the individual member states.\textsuperscript{107}

The “Data Subjects’ Bill of Rights” places a large burden on the processor and the controller of data. It empowers individuals to protect themselves against physical and electronic invasions of their Privatsphäre. If no such rights exist, these individuals must bear all damages related to the invasion of their personal privacy. However,

\textsuperscript{96} Such information includes “the existence of a processing operation, its purpose, the categories of data concerned, any third parties . . . to whom the data are to be disclosed, and the name and address of the controller . . . .” \textit{Id.} art. 10(1).

\textsuperscript{97} \textit{Id.} art. 11(1). This includes the purpose for the processing of data, whether the reply to any questions posed by the processor is voluntary or mandatory and any consequences for noncompliance, the data user, any existing rights to access to the data collected, and the name and address of the data controller. Public authorities are exempted from this requirement. \textit{Id.} art. 11(2).

\textsuperscript{98} \textit{Id.} art. 12(1).

\textsuperscript{99} \textit{Id.} art. 12(2).

\textsuperscript{100} \textit{Id.} art. 13(1). Any member state may restrict this right to protect paramount interests, such as national security, criminal proceedings, public safety, and others. \textit{Id.} art. 14(1).

\textsuperscript{101} \textit{Id.} art. 13(3).

\textsuperscript{102} \textit{Id.} Once such erasure or blocking has occurred, the data subject must be notified. \textit{Id.} art. 13(4).

\textsuperscript{103} \textit{Id.} art. 15.

\textsuperscript{104} \textit{Id.} art. 22.

\textsuperscript{105} \textit{Id.} art. 23(1).

\textsuperscript{106} \textit{Id.} art. 23(2).

\textsuperscript{107} \textit{Id.} art. 24.
besides having an incentive to comply, the processors and controllers of data are collectively able to spread the cost of compliance among their customers; this is a luxury not available to the individual.

5. Transborder Data Flows

Both the OECD Guidelines and the European Convention used the test of "equivalent data protection laws" when determining whether personal data should be sent across national borders;\(^{108}\) under these guidelines, however, the exact standard of equivalency was never determined. While both the 1990 Proposal and the Amended Proposal of 1992 provide that each member state must assure that personal data are transmitted to a third nation for the purpose of processing only if that receiving nation "ensures an adequate level of protection,"\(^{109}\) neither proposal includes a definition of equivalency.

After much debate before the European Parliament, and on the recommendation of the Economic and Social Committee,\(^{110}\) this fairly high standard was relaxed in the Amended Proposal, which made transfers possible under certain conditions, even if the recipient nation did not possess such an adequate level of protection.\(^{111}\) Under the Amended Proposal, the member nations themselves are charged with reporting third nations that do not have adequate levels of protection to the Commission,\(^{112}\) so that the Commission may negotiate remedial measures with the offending nation.\(^{113}\)

The standards for transborder data flows to third nations are still very high, having long raised concerns among many businesses and commentators.\(^{114}\) However, a lack of strict standards would render the directives useless, since businesses could simply "export" personal data to non-European nations and process these data outside the reach of European data protection directives and national data protection laws.

108. Most nations have developed the practice of following the equivalency standard. See Pearson, supra note 5.

109. Amended Proposal, supra note 6, art. 26(1).

110. See Economic and Social Committee Opinion, supra note 63, ¶ 2.2.19.

111. Amended Proposal, supra note 6, art. 26(1). The Amended Proposal makes such a transfer possible if the data subject consents, if a contract to do so exists between the data subject and the controller, if the transfer is necessary to further an important public interest, or if "the transfer is necessary in order to protect the vital interests of the data subject." Id. art. 26(1). These provisions eliminate some of the vagueness about which critics of the 1990 proposal complained. See Estadella-Yuste, supra note 60, at 175-77.

112. Amended Proposal, supra note 6, art. 26(3).

113. Id. art. 26(4).

114. See, e.g., David P. Farnsworth, Data Privacy or Data Protection and Transborder or Transnational Data Flow, an American’s View of European Legislation, 11 Int’l Bus. Law. 114 (1983).
B. The 1994 Network Draft

The European Commission intended the Original Network Draft of 1990 to operate independently of the other two proposals; the Commission changed its approach for the Network Draft of 1994 to supplement the Amended Proposal of 1992 in the area of telecommunications. Some of the Network Draft’s provisions overlap with those of the Amended Proposal and are not discussed here.

Specifically, the Network Draft addresses telecommunications organizations, public telecommunications services, and the provider of such services. All data must be kept confidential, notwithstanding distribution with the subscriber’s consent; the service provider may not make “the provision of its service dependent upon such consent.” The Commission was especially concerned that data incidental to the use of such services be stored and used only for billing purposes; the service provider must destroy such data as soon as they become outdated for that purpose. Today’s technology allows network providers, such as America Online, to easily monitor an individual’s account and keystroke activity. For instance, by monitoring certain meeting rooms, such providers can easily assess a person’s

---

115. Network Draft, supra note 67. For the nature of this streamlining effort, see id. at 7-11.
116. The Network Draft defines “telecommunications organizations” as:
[A] public or private body, to which a Member State grants special or exclusive rights for the provision of a public telecommunications network and, where applicable, public telecommunications services.
Id. art. 2(1)
117. A “public telecommunications service” is a “telecommunications service whose supply Members States have specifically entrusted inter alia to one or more telecommunications organizations.” Network Draft, supra note 67, art. 2(6). A “public telecommunications network,” on the other hand, is a “public telecommunications infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means.” Id. art. 2(5).
118. Id. art. 3. The Network Draft defines such a service provider as “a natural or legal person providing services whose provision consists wholly or partly in the transmission and routing of signals on a public telecommunications network, with the exception of radio broadcasting and television.” Id. art. 2(2). The latter exception is a bit troublesome given the recent diminution of differences between, for instance, cable television and electronic information services. In Europe, videotext/teletext has already made that line very indistinguishable.
119. Id. art. 7(1) and (2). A subscriber is defined as “any natural or legal person having subscribed to a telecommunications service of a telecommunications organization or another service provider.” Id. art. 2(3).
120. Id. art. 7(3).
121. Id. art. 5. See also id. art. 6 (addressing electronic “traffic” data incidental to the provision of services to the subscriber). These provisions apply especially for itemized bills. Id. art. 7. (In Europe, unlike in the United States, itemized billing, for instance, for telephone calls, is still relatively rare as many consider such a service extravagant.)
122. Id. art. 7.
political, sexual, and other preferences. Such technology makes protective regulations such as the ones proposed in this article a necessity.

In respect of protective regulations, the Network Draft specifically addresses telephone services, often restricting the use of day to day services that Americans have long taken for granted. For instance, telephone calls may only be forwarded to a third party if that party agrees;\textsuperscript{123} telephone directories may only list identifying information that is absolutely necessary to identify the subscriber.\textsuperscript{124} In addition, telephone subscribers must be given the option to block caller identification.\textsuperscript{125} Telephone subscribers have the right not to receive solicitations if they so desire;\textsuperscript{126} this applies also to pre-recorded voice\textsuperscript{127} as well as fax solicitations.\textsuperscript{128} Furthermore, member states must assure that telephone tapping devices are kept out of public hands and are applied by authorized governmental agencies only, "subject to authorization by the competent judiciary or administrative national authorities in conformity with national legislation."\textsuperscript{129} Once conversations are recorded, the contents must remain confidential and may not be relayed to unauthorized third parties.\textsuperscript{130} For that reason, the Commission compels service providers to provide their subscribers with encryption facilities upon request for mobile phones to prevent interception via airwaves.\textsuperscript{131}

Again, individuals are given private rights of action to recover any damages suffered from violation of the Network Draft.\textsuperscript{132} In addition, the working party as established under the Amended Proposal will oversee proper implementation of the Network Draft.

Overall, the Amended Proposal and the Network Draft provide a very competent set of rules in favor of personal data protection. These rules are very general and will require some time for implementation, but this burden is reduced by the fact that most European nations already have strong data protection laws; those nations will merely have to streamline their regulations to comply with the European direc-

\textsuperscript{123} Id. art. 10.
\textsuperscript{124} Id. art. 11.
\textsuperscript{125} Id. art. 8.
\textsuperscript{126} Id. art. 13(1).
\textsuperscript{127} Id. art. 13(2).
\textsuperscript{128} Id. art. 13(3).
\textsuperscript{129} Id. art. 12(1).
\textsuperscript{130} Id. art. 12(2).
\textsuperscript{131} Id. art. 4. The number of impositions of "technical" solutions, such as this one, has been reduced from the Original Network Draft. See Spicers Centre for Europe, Amended Draft Directive on Personal Data Protection, June 13, 1994, available in LEXIS.
\textsuperscript{132} Network Draft, supra note 67, art. 16.
These directives will certainly reduce the anxiety felt by many Europeans about the "publication" of their private lives.

IV. DATA PROTECTION IN THE UNITED STATES

Unlike under the European Commission, no comprehensive regulations favoring an individual's right to privacy exist in the United States. The American law has been very slow to respond to the challenges of data protection presented by the information age.134 This is quite an interesting phenomenon, since in 1890 two Americans, Warren and Brandeis, first identified privacy as the right to be left alone from the intrusions of the state and other individuals.135 This section discusses briefly the historical development of data protection in the United States, followed by a brief summary of shortcomings.

A. The United States Constitution and the Supreme Court

Authorities agree, so it appears, that there are at least two types of privacy that are rooted in the Constitution. The First Amendment recognizes a person's right to privacy in cases when one person's speech collides with another's freedom of thought and solitude.136 The Fourth Amendment establishes that an individual is free from government searches and seizures.137 The Constitution addresses some privacy issues, but does not explicitly recognize a right to privacy, let alone data privacy. However, the European proposed directives on data protection take a comprehensive approach to protecting the individual.138

Privacy principles have been introduced in many Supreme Court cases.139 In Roe v. Wade, these principles were based on the Four-
teenth Amendment.\textsuperscript{140} The Court, however, has been hesitant to extend the constitutional rights of privacy to the area of data protection. For instance, in \textit{Paul v. Davis}, the Court held that the right to nondisclosure of personal information is not a fundamental right as is the privacy right to procreation,\textsuperscript{141} unless this disclosure affects a fundamental right.\textsuperscript{142} However, in \textit{Whalen v. Roe}, the court recognized in dicta that the there may exist a right to protect against improper disclosure of personal data.\textsuperscript{143} However, the Court in that case held that the law in question did not violate the complainant's privacy rights.\textsuperscript{144}

These few decisions notwithstanding, the Court acted on the understandable desire to leave tort legislation to Congress or to the common law of the states. Acts of Congress and common law are discussed next.

\textbf{B. Acts of Congress}

Congress has taken “a sectoral, device specific, and activity or damage specific” approach to data protection;\textsuperscript{145} this approach may be popular with Congressional lobbyists with deep pocket clients, but it does not further the individual’s cause of informational privacy.

The first statutory protection of data dissemination was ratified in the Fair Credit Reporting Act of 1970 [FCRA].\textsuperscript{146} The FCRA provides specific rights for individuals and places responsibilities on credit reporting agencies with respect to an individual’s credit worthiness.\textsuperscript{147} The data reported must be accurate and up to date,\textsuperscript{148} and the individual has the right to correction,\textsuperscript{149} thereby somewhat preceding the European Convention.\textsuperscript{150} However, the FCRA only deals with data dissemination, not with data collection or storage.\textsuperscript{151} While credit bureaus must assure that the captured data are accurate, they are not held strictly liable for errors;\textsuperscript{152} in reality, the burden remains on the individual to show that the data are incorrect.\textsuperscript{153}

\begin{itemize}
\item \textsuperscript{140} 410 U.S. 113 (1973).
\item \textsuperscript{141} 424 U.S. 693, 713 (1976).
\item \textsuperscript{142} \textit{Id.} at 713-14.
\item \textsuperscript{143} 429 U.S. 589, 605 (1977).
\item \textsuperscript{144} \textit{Id.} at 605-06.
\item \textsuperscript{145} Boehmer and Palmer, \textit{supra} note 138, at 303.
\item \textsuperscript{146} 15 U.S.C. §§ 1681-81t (1988).
\item \textsuperscript{147} \textit{Id.} § 1681(b).
\item \textsuperscript{148} \textit{Id.} §§ 1681e(b), 1681k(2).
\item \textsuperscript{149} \textit{Id.} § 1681i.
\item \textsuperscript{150} See \textit{supra} part II.B.
\item \textsuperscript{152} 15 U.S.C. § 1681e.
\item \textsuperscript{153} \textit{Id.} § 1681.
The Privacy Act of 1974\textsuperscript{154} represents Congress' first comprehensive approach to the protection of individuals' data as collected, stored, and disseminated in the public sector. Notwithstanding twelve exceptions,\textsuperscript{155} the federal government may not disclose personal data without consent of the data subject.\textsuperscript{156} An individual may have false information corrected and has the right to access his file.\textsuperscript{157} Perhaps most important, the Privacy Act of 1974 requires the government to exercise due care in the compilation of personal data and to have controls that secure databases from unauthorized access.\textsuperscript{158} However, the Privacy Act of 1974 applies only to governmental data bases.\textsuperscript{159} Private data gatherers are not covered by this Act. In addition, while the Act covers data dissemination, it does not address improper gathering of data, nor does it address data quality issues.

To supplement the Privacy Act of 1974, the legislature passed several additional laws, such as the Fair Credit Billing Act of 1974,\textsuperscript{160} which provided individuals with the right of error correction in false credit card statements.\textsuperscript{161} The Equal Credit Opportunity Act of 1974\textsuperscript{162} prohibits the consideration of sex, race, color, religion, national origin, age, or marital status when granting credit and requires credit institutions to provide the credit seeker with specific reasons for denial.\textsuperscript{163} However, both statutes place the burden of proving errors on the individual; until called to the attention of the controller of data, no duty exists to gather correct information and to update that information.

Public school records are protected from dissemination to third parties under the Family Education Rights and Privacy Act of 1974.\textsuperscript{164} Again, this Act does not address error correction or disposal of old data.

The Electronic Funds Transfer Act of 1978\textsuperscript{165} requires banks to make disclosures to a party, whose account is debited, as to the nature of the debit.\textsuperscript{166} This statute is so narrow in scope that its impact is

\begin{itemize}
\item \textsuperscript{154} 5 U.S.C. § 552a.
\item \textsuperscript{155} Id. § 552a(b)(1)-(12) (1988 & Supp. 1993).
\item \textsuperscript{156} Id. § 552a(b) (1988).
\item \textsuperscript{157} Id. §§ 552a(d)(1), (d)(2)(B)(i).
\item \textsuperscript{158} Id. §§ 552a(e)(9), (e)(4)(E), (e)(5).
\item \textsuperscript{159} Id. § 552a(b).
\item \textsuperscript{160} 15 U.S.C. § 1601-67(e).
\item \textsuperscript{161} Id. § 1666.
\item \textsuperscript{162} Id. §§ 1691-1691(e) (1988 & Supp. 1993).
\item \textsuperscript{163} Id. § 1691(d).
\item \textsuperscript{164} 20 U.S.C. § 1232g(b) (1988).
\item \textsuperscript{165} 15 U.S.C. §§ 1693–93r.
\item \textsuperscript{166} Id. § 1693d.
\end{itemize}
almost negligible. For instance, it does not address dissemination of
general account history. Along similar lines, the Right to Financial
Privacy Act of 1978\(^\text{167}\) requires financial institutions to notify their
customers before information is provided to government agencies.\(^\text{168}\)
The statute is silent on the distribution of the customer’s name to
telemarketing and other intrusive agencies.

The Privacy Act of 1980\(^\text{169}\) prohibits government agents from
seizing the work product of the media. This law was passed in direct
response to the raid in question in Zurcher v. Stanford Daily.\(^\text{170}\) The
statute reemphasizes the conflict between governmental pursuit and
the media’s right to know. Zurcher reduced individuals’ rights in that
the government is not allowed to seize materials to prosecute criminal
libel cases; this leaves the individual only with civil remedies.

The Electronic Communications Privacy Act of 1986\(^\text{171}\) criminally
prohibits wiretapping. However, the Act permits phone companies
to capture necessary billing data, such as the recipient’s phone
number; the Act also does not regulate use and dissemination of that
billing data.\(^\text{172}\) The Act does not specifically address the issue of data
protection for cases in which modems communicate confidential data;
however, it appears that wiretapping to intercept any type of commu-
nication is prohibited.

The Cable Communications Policy Act of 1984\(^\text{173}\) requires that
cable operators notify customers if personally identifiable data about
these consumers are to be collected.\(^\text{174}\) The individual also has the
right to know the purpose of the data collection and the duration of
data storage.\(^\text{175}\) Written or electronic consent must precede disclosure
of subscriber specific information to third parties.\(^\text{176}\) However, ser-
vice agreements that condition the providing of service on such con-
sent can easily circumvent this statute’s provision.


\(^{168}\) Id. § 3402 (except if the request is a subpoena or search warrant).


\(^{172}\) Reidenberg, supra note 151, at 215.


\(^{174}\) Id. § 551.

\(^{175}\) Id. § 551(a)(1)(A) and § (C).

The Video Privacy Protection Act of 1988 provides for civil action against video renters for dissemination of a customer's renting history. In this most recent statement on data protection, Congress did address all processing activities; however, that Act is limited only to the home entertainment sector.

C. Common Law

Unless a specific aspect of privacy legislation is addressed by one of the above federal acts, an individual must rely on tort law. First, an "intrusion upon the individual’s physical solitude or seclusion" may involve data disseminated without the data subject’s consent to a third party. Second, such disclosure also involves the tortious public disclosure of private facts. Both torts have been recognized by various courts.

It is also possible that a person’s personal data are considered property. While property is defined as an interest recognized by the law, that recognition has not yet taken place for personal data. Until the law recognizes such a right, one must argue that personal data fall under the type of intellectual property now protected at the federal level. To date, the federal government will not grant a corporation a copyright on the white telephone pages, even if that company went through sufficient efforts in making the telephone white telephone pages useful. It appears that Congress is far away from recognizing a property interest in an individual’s personal data.

Last, an individual may contract with a processor of data to not publish the individual’s information, if the data processor disseminates such data, he is in violation of his contract and must pay damages to the individual. However, contract law does not allow punitive damages; this results in the benefits of noncompliance far too often outweighing the cost of breach. The result is a contract breach in which the individual is paid for the value of nondissemination while

178. Id. § 2710(C).
179. Reidenberg, supra note 151, at 220.
181. Blackman, supra note 180, at 446-47.
182. Id. at 446-47.
183. Id. at 450.
185. See Blackman, supra note 180, at 450-52.
the individual’s personal information has become known to millions.\textsuperscript{186}

V. FILLING THE VOID OF DATA PROTECTION IN THE UNITED STATES: FOLLOWING THE EUROPEAN EXAMPLE

Based on the above, it is clear that U.S. laws do not adequately protect an individual in the area of data privacy. This is because Congress has never consistently treated privacy concerns. The narrow and haphazard assortment of privacy rights through legislation and common law doctrines neither respond coherently nor consistently to data protection concerns.\textsuperscript{187} The operative term here is \textit{prescribe}. Congress has never \textit{prescribed}.

This leaves U.S. corporations subject to market disadvantages. The European Commission requires that if data are to be moved outside the Union, the controller must be satisfied that the receiving country has adequate safeguards in place; traditionally this adequacy has been defined as “equivalency.” However, equivalency simply does not exist. The United States does not have the equivalent to the supervisory board as required by the Amended Proposal.\textsuperscript{188} The United States also does not “provide the collection-to-erasure style protection” of the Amended Proposal.\textsuperscript{189} As a result, the controller is not likely to permit data to be moved to the United States. This could force U.S. companies to keep two separate data bases, significantly reducing the achieved economies of scale.\textsuperscript{190}

The present approach to data protection in the United States must change. Broad Congressional legislation protecting informational privacy is needed both to protect individuals and to serve commercial interests.\textsuperscript{191} At the same time, however, a workable balance must be struck between the needs of the individual and the needs of the enterprise.\textsuperscript{192}

One commentator proposed a piece of legislation that addresses the private sector’s use of personal data.\textsuperscript{193} The commentator’s “Pri-
Private Sector Privacy Act" follows some of the principles set out by the Amended Proposal. It calls for a data protection board which, similar to the supervisory board, oversees proper application of the rights to privacy.\(^\text{194}\) In addition, the proposed statute prohibits the collection and disclosure of an individual's data without consent and places the burden of correcting data on the controller.\(^\text{195}\) It also provides a bill of rights of data subjects similar to those articulated in the Amended Proposal.\(^\text{196}\) However, the proposed statute would also apply to illegal aliens, a group of people he excludes from the proposed statute's protected class.\(^\text{197}\) While this statute presents a good start, it also does not apply to governmental uses of data.

This author has the following recommendations to drafters of privacy legislation. First, a statute should cover all types of personal data, gathered manually or electronically by governmental agencies, businesses, and nonprofit entities.

Second, the controller of the data must ascertain that the individual's privacy is adequately protected; such a provision would keep the types of data collected to the absolute minimum necessary for accomplishing the purpose for which the data were gathered. The controller must ascertain that any personal data are securely stored and, using the highest standard of care, that information is not accessed without authorization. This places the burden on the controller to ascertain that unwanted hackers cannot gain access to the computer system, potentially invading the data subject's privacy.

Third, a governmental body through the exercise of the commerce power, essentially a "data police," should be charged with nationwide implementation and enforcement of the statute's provisions.\(^\text{198}\) This prevents larger corporations from shopping for states with the least rigorous rules from which to gather and in which to process personal data.

Fourth, the statute should establish strict data quality standards. Data should not be gathered unless the individual is notified of all purposes for which the data are collected and unless the individual has given consent to such gathering and processing. Critical data, such as medical data, sexual preferences, race, religious, political, and philosophical views, should be destroyed unless the data subject has given written consent for each three month period in which the data are to be

\(^{194}\) Id. at 466.

\(^{195}\) Id.

\(^{196}\) Id. at 467-68.

\(^{197}\) Id. at 466.

\(^{198}\) George Trubow, Protecting Informational Privacy in the Information Society, 10 N. Ill. L. Rev. 521, 530 (1990).
used. In addition, insurance companies, financial institutions, and other service providers should under no circumstances be allowed to make an individual’s receipt of service dependent on the individual’s consent.

Fifth, personal data should not be distributed to any third parties unless the data subject has given written consent. Exceptions, to be used rarely and judiciously, should be made for pressing national security interests.

Sixth, this author proposes a data subject’s bill of rights similar to that introduced in the Amended Proposal’s Bill of Rights, including the right to know what data are captured for which purpose, the right to consent and withdraw consent and the right to rectify or erase false information.

Seventh, transborder data flows should be prohibited unless the recipient country legislatively protects such personal data adequately. Such a provision would prevent circumvention of the proposed statute by way of establishing a subsidiary in a “data controller-friendly country” for the sole purpose of storing and disseminating data which would otherwise be prohibited under such statute.

Eighth, the data subject should be granted a private right of action for violations of the provisions of this statute. The statute should set the standard of highest care on the controller of data, holding him strictly liable for violations of the statute. Such a high burden is justified since the controller of data is in the only position to fairly process personal information. Criminal penalties on the corporation and its management board should be provided for knowing violations of the statute’s provisions.

The above proposals restrict a business’s ability to use personal data. Such a statute would tremendously increase the cost of keeping personal information. However, if spread over 250 million inhabitants, the incremental costs of products and services is likely to be negligible compared to the exposure to which an individual is subjected under the present system of noninterference when making a simple telephone call to place a request on one of America Online’s bulletin boards. The range of the burden presently on the individual is as high as the potential for abuse and blackmail and as low as receiving solicitation telephone calls.

VI. OBSERVATIONS AND CONCLUSIONS

It is clear that at present the law in the United States does not recognize individual’s personal data as an interest that needs to be protected. This is an interesting phenomenon since the founders of the
United States emigrated from governmental systems that did not recognize their rights — the right to free exercise of religion, the right to free speech, and the right to be left alone. While American lawmakers have done an excellent job protecting the first two of these rights, they have neglected the third. The increase in cost of doing business is one obvious reason for this neglect. Cynics would point out that Washington serves its industrial constituents by purposely looking the other way. While some of that cynicism may be justified, one must point out, in all fairness, that Congress has had numerous occasions on which to contemplate legislation that would substantially advance an individual’s right to have data pertaining to him remain his own.\textsuperscript{199}

The Europeans, on the other hand, have advanced laws protecting personal data since the 1970s. The Amended Proposal together with the Network Directive possibly represent the state of the art in privacy protection. Future plans to incorporate privacy in the information society are already underway.\textsuperscript{200} Congressional action incorporating some of these provisions in a comprehensive data privacy statute would better assure the protection of U.S. residents' rights to privacy.

If Europe is willing to enforce the Amended Proposal's transborder data flows provisions, it may indirectly effect a change in U.S. law as well. Such a change will occur as soon as American multinational corporations are prevented from exporting European data to the United States because of inadequate U.S. regulation, thereby increasing the costs and reducing the profits of those corporations.

Nothing will force Congress to act quickly as will the plea of the corporate constituency. Consequently, a changed approach to data protection appears inevitable in the United States; only time will tell how quickly such a change will occur. The sooner such change occurs, the better.
