Creating Data Protection Legislation in the United States: An Examination of Current Legislation in the European Union, Spain, and the United States

Jennifer M. Myers

Follow this and additional works at: https://scholarlycommons.law.case.edu/jil
Part of the International Law Commons

Recommended Citation
Available at: https://scholarlycommons.law.case.edu/jil/vol29/iss1/3
CREATING DATA PROTECTION LEGISLATION IN THE UNITED STATES: AN EXAMINATION OF CURRENT LEGISLATION IN THE EUROPEAN UNION, SPAIN, AND THE UNITED STATES

Jennifer M. Myers*

I. INTRODUCTION

THE EVOLUTION AND USE OF INFORMATION TECHNOLOGY¹ in the last decade have caused the legal world to reconsider how its methods and structures affect an individual’s privacy rights.² Advances in information technology³ contribute to increasing amounts of electronically stored personal data,⁴ processing of personal data in various spheres of social and economic activity,⁵ and the ability to access that data.⁶ Such data

* B.A. 1994, Colgate University; J.D. Candidate, May 1997, Case Western Reserve University School of Law. The author wishes to thank Professor Christine Corcos for her suggestions and guidance.

¹ Information technology is generally understood as the “[s]cience of the automatic treatment of information.” MIGUEL ÁNGEL DAVARA RODRIGUEZ, DERECHO INFORMATICO 23 (1993) [hereinafter DERECHO INFORMATICO] (translation by author).

² See id. at 24. These advances also trigger questions regarding whether governments, businesses, and individuals should protect these rights, and if so, how.

³ Advances occur in areas such as artificial intelligence, relational databases, interactive telecommunications, and distributed data processing. See WAYNE MADSEN, HANDBOOK OF PERSONAL DATA PROTECTION 3 (1992).

⁴ See id. “Information” as a concept concerns the meaning assigned to or derived from data or the total meaningful content of data. See Jon Bing et al., Legal Problems Related to Transborder Data Flows, in AN EXPLORATION OF LEGAL ISSUES IN INFORMATION AND COMMUNICATION TECHNOLOGIES 59, 69 (1983). “Data” is defined as “information recorded in a form in which it can be processed.” MADSEN, supra note 3, at 202.


⁶ See MADSEN, supra note 3, at 2; The European Commission: Developing the Legislative Framework for the Information Society, M2 Communications Presswire, Oct. 6, 1995, available in 1995 WL 10868989 (stating that new media such as electronic storage facilitate the storage and management of the increasing amount of printed material and volumes of information) [hereinafter Legislative Framework].

109
can reveal numerous characteristics about a person's identity, including medical history and financial stability.\(^7\) Technological advances in this area have not been accompanied simultaneously by a social respect for the stored and transmitted data.\(^8\) As a result of the limited social respect for electronically stored data, amounts of data stored, and ability to easily access information,\(^9\) individuals, groups, and governments are concerned that this storage threatens personal privacy.\(^10\) Increased data storage as well as easy accessibility and manipulability of stored data prevent individuals from controlling the dissemination of information about themselves.\(^11\) The common belief that the possessor of such information holds the key to power\(^12\) complicates the creation of effective data protection legislation because it is no longer a question of who possesses the information, but instead, who knows how to manage and manipulate

\(^7\) See MADSEN, supra note 3, at 202.

\(^8\) See DERECHO INFORMÁTICO, supra note 1, at 48 (commenting on the degree to which personal information has become computerized and thus subject to outside scrutiny). These abuses occur in data stored by both the private and the public sector. See infra 171-81 and accompanying text.

\(^9\) Even individuals with limited computer knowledge can access databases, manipulate data, and, in effect, exercise control over the person whose data they have changed. See MADSEN, supra note 3, at 2-3 (discussing how personal data can be entered by a mere telephone call).

\(^10\) See DERECHO INFORMÁTICO, supra note 1, at 48. When data is stored electronically it is susceptible to access and use beyond the purpose for which it was originally obtained. See, e.g., John Markoff, Ideas and Trends; Remember Big Brother? Now He's a Company Man, N.Y. TIMES, Mar. 31, 1991, at § 4, 7 (discussing companies' uses of technological advancement to gather information on potential employees and customers); ALBERT GORE, JR. & RONALD H. BROWN, GLOBAL INFORMATION INFRASTRUCTURE: AGENDA FOR COOPERATION 23 (1995) (discussing the serious violations of privacy or property rights that can occur by distorting or destroying information. Even individuals in remote locations can use their computer terminals to cause violations to others). All of this data manipulation can occur without the affected individual's knowledge. See MADSEN, supra note 3, at 2-4.

\(^11\) See, e.g., Amanda Hoey, An Ethical Issue of the Information Age — Computers and Privacy, 11 COMPUTER L. & PRAC. 126 (1995) (discussing that privacy in terms of data collection, manipulation, and storage falls within the classification of information privacy). Information privacy is primarily concerned with an individual's ability to control the circulation of information pertaining to himself or herself. With the increasing amount of information stored electronically and the amount of information manipulated and sold to others, individuals cannot know exactly where and what information is circulating about themselves. See id.

\(^12\) DERECHO INFORMÁTICO, supra note 1, at 24.
the information. These concerns form the basis of discussions surrounding data protection measures.

As early as the 1960s, the United States recognized dangers inherent in storing large amounts of personal information. The United States enacted the Privacy Act of 1974 and the Freedom of Information Act to control the dissemination of information stored in federal data banks. However, these acts have not curtailed the misuse of electronically stored personal information. Consequently, the United States

---

13 See id.

14 It should be mentioned at the outset that data protection is distinct from data security. In general, data security refers to physical or organizational measures that can be implemented to prevent access or destruction to contents. For a discussion of data security, see, e.g., DAVID H. FLAHERTY, DATA SECURITY AND GOVERNMENT DATA BANKS: AN INTERNATIONAL PERSPECTIVE (1979).

15 With the expansion of the number of databases came the increasing collection, storage, and movement of personal data. For example, the market for databases increased from 10,000 customers in 1965 to two million customers in 1978. The customers included national and multinational corporations, as well as governmental and quasi-governmental institutions. See Hon. Mr. Justice M.D. Kirby, Legal Aspects of Information Technology, in ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT; INFORMATION COMPUTER COMMUNICATION POLICY 18 (1983) (discussing a study by O.H. Ganley & G.D. Ganley, To Inform or to Control?, in THE NEW COMMUNICATIONS NETWORKS 85-86 (1982)).


18 See MADSEN, supra note 3, at 107. The Privacy Act of 1974 and the Freedom of Information Act cannot curtail the misuse of data in part because they only regulate data stored by the public sector. At present there is a shift from government entities to private sector firms as the collector and user of personal data. See GORE & BROWN, supra note 10, at 21 (stating that during the 1970s and 1980s, businesses took advan-
adopted a sectoral approach to safeguarding an individual's right to privacy in stored information by regulating particular abuses as they arose. However, this sectoral legislation also cannot adequately address privacy concerns. Therefore, in light of the treatment and importance of personal information throughout the world, the United States should create comprehensive national data protection legislation. Doing so will protect an individual's right to privacy in electronically stored data and secure the unhampered role of the United States in the world market.

While the United States has been unable to pass comprehensive data protection legislation, the European Union has addressed this issue by passing a Directive regulating the processing of personal data. In consideration of this legislation, E.U. Member States adopt (or create if

tage of the growth of low-cost, high-performance computers and adapted the technology to a wide range of economic, financial, and marketing applications). Additionally, these acts were unable to adequately balance the privacy of information with adequate disclosure. See infra part IV.

20 See, e.g., Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1996 Supp.) (designed to address computer-related crimes, such as unauthorized computer access); Video Privacy Protection Act, 18 U.S.C. § 2710, 2711 (1988) (preventing wrongful disclosure of video tape rental or sale records. Video tape renters or sellers cannot disclose the identity of individuals renting tapes or the particular tapes rented; however, renters can release mailing lists of their customers that show the category of videos rented, but not the specific titles except in limited circumstances. This act also provides the consumer with a grievance procedure against the seller or renter.); Fair Credit Reporting Act of 1988, 15 U.S.C. § 1681 (1988) (providing a structure for the use of matching between government agencies and departments). This piecemeal approach to data protection cannot adequately protect an individual's privacy rights, or prevent abuses. See infra part IV.

21 See infra part IV. See also Boehmer & Palmer, supra note 5, at 265 (discussing the importance of trans-border data flows for international businesses).

necessary) laws to conform to the Directive. One country in particular, Spain, merits attention because its constitution specifically grants its citizens a right to privacy in electronically stored information. Premised on the Spanish Constitution's explicit guarantee that "the law will limit the use of information in order to safeguard the honor and privacy of the person and the family of citizens and the full exercise of their rights," the Spanish Parliament passed an Act entitled the "Law on the Regulation of the Automated Processing of Personal Data" (LORTAD) in February 1992. In delineating the extent of protection, LORTAD attempts to balance competing interests between the access to information and the right to privacy.

In light of the recent passage of the E.U. Directive, Member State laws conforming with the Directive, economic implications for the United States, and threats to personal privacy that result from the misuse of data, the United States must enact comprehensive data protection legislation conforming with the E.U. Directive to ensure its continued participation in the global market. The European Union and the United States are each other's largest trading and investment partners, and each relies on the transfer and storage of large amounts of personal information. Cross-border flows of personal data are necessary for the expansion of international trade, and are capable of shaping the world's economic system. Although E.U. Member States rely on the transfer of data from

---

23 Council Directive, supra note 22, ¶ 69. Member States have three years to apply the Directive to their national rules; the Directive allows Member States twelve years to ensure that manual files within the state conform to the Directive. Id.

24 Constitución [constitution] art. 18.4 (Spain).

25 Id.


27 Id. at Exposición de Motivos § 4.


29 See Council Directive, supra note 22, ¶ 6 (stating that "the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data.").

30 See GORE & BROWN, supra note 10, at 3 (reporting Gore's statement during a speech given at the International Telecommunications Union World Development Conference in Buenos Aires, Argentina in March 1994). Vice President Gore introduced the Clinton Administrations's vision for a Global Information Infrastructure (GII) and emphasized the importance of information throughout the world. Information is rapidly created, easily accessible, and most importantly useful; it is therefore capable of causing fundamental changes in each nation's economy. See id.
other nations, the E.U. Directive precludes those nations that do not have adequate data protection from receiving data, specifically those nations that do not have adequate privacy protection for their citizens in electronically stored data.\(^{31}\) Some E.U. Member States have already expressed concerns that the United States does not have adequate data protection legislation.\(^{32}\) Therefore, the United States should adopt comprehensive data protection legislation immediately. As the global market and information technology systems continue to grow, and the number of database users and controllers increases, regulating the storage, transfer, and collection of data will become increasingly difficult.\(^{33}\) At the same time, countries will become more dependent on this data,\(^{34}\) and the United States should not risk being precluded from receiving data because it does not have adequate levels of individual privacy protection.\(^{35}\)

Part II of this Note examines the E.U. Directive and the regulations preceding the adoption of the Directive.\(^{36}\) Part III examines LORTAD, the recently passed Spanish data protection law,\(^{37}\) and discusses Spain’s approach to balancing the constitutional guarantees of the right to privacy and freedom of information. Part IV demonstrates that there are compelling reasons for the United States to create comprehensive national data

\(^{31}\) Council Directive, \textit{supra} note 22, art. 25. According to the principles articulated in Article 25, “Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if . . . the third country in question ensures an adequate level of protection.” \textit{Id.} art. 25 ¶ 1. For a discussion of the effect of regulations regarding data protection and transborder data flows on multinational enterprises, see e.g., Boehmer & Palmer, \textit{supra} note 5, at 265.

\(^{32}\) \textit{See} Mitch Ratcliffe & Mitzi Waltz, \textit{Easing Data Transfer Across Borders; European Laws Can Present Roadblocks}, MACWEEK, Nov. 2, 1992, at 20. Although the United States is a large trading partner with E.U. Member States, that status will not prevent Member States from preventing the transfer of data to the United States. The author notes that several Member States have already expressed concerns that the United States does not have adequate levels of data protection. \textit{See id.}


\(^{34}\) Gore & Brown, \textit{supra} note 10, at 23.

\(^{35}\) \textit{See} Ratcliffe & Waltz, \textit{supra} note 32, at 20 (discussing that European countries do not believe that the United States has adequate data protection legislation). The United States has already been precluded from receiving certain information. For example, Sony Germany cannot export consumer data to the United States because of the lack of stringent U.S. privacy safeguards. \textit{See id.}


protection legislation. Such reasons include preventing abuses and the misuse of data, protecting personal privacy, and ensuring continued U.S. participation in the world market. By protecting an individual's right to privacy in electronically stored information, the United States will be able to continue actively participating in the world market. Furthermore, Part IV explains that existing constitutional guarantees and piecemeal legislation are unable to protect an individual's right to privacy in electronically stored information. Finally, Part IV examines current barriers to creating U.S. data protection legislation like the desire to balance access to information with the right to privacy. In doing so, the section draws upon Spain's success in overcoming these barriers. Part V concludes that sufficient incentives exist for the United States to create data protection legislation and that such legislation will not frustrate constitutional mandates in the U.S. Constitution.

II. THE E.U. DIRECTIVE AND PRIOR DATA PROTECTION LEGISLATION

A. Introduction

On July 25, 1995, the European Union's sixteen Member States, in accordance with the objectives of the European Union, formally ap-

38 Admittedly, the concept of privacy is different throughout the various nations of the world. It will be distinct among nations, social levels, and cultures among other qualifying criteria; however, these differences are insufficient barriers to suppress U.S. creation of data protection legislation.

39 See Kirby, supra note 15, at 22. Information has been regarded as the "currency of democracy," and therefore legislatures were initially forced to tread carefully when proposing to curtail the flow of information. Id. Creating effective legislation in the United States, as well as in other countries, revives the struggle to balance the right to information and the right to privacy. See, e.g., ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, PRIVACY AND DATA PROTECTION: ISSUES AND CHALLENGES (1994) (report prepared according to the OECD Guidelines of September 23, 1980, implementing a regulation that the Secretariat of the Committee on Information, Computer and Communications Policy (ICCP) would conduct a survey to determine present trends in privacy and data protection in Member Countries and the extent to which the Recommendation has been followed) [hereinafter PRIVACY AND DATA PROTECTION].

40 The E.U.'s sixteen Member States include Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, and the United Kingdom.

41 According to the Treaty on European Union, the objectives of the European Union include: establishing an even closer union among the people of Europe, fostering closer relations between the States belonging to the Union, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of the people, preserving and strengthening peace
proved the "Common Position on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data" (E.U. Directive).\textsuperscript{42} Responding to the threats that an individual's personal privacy could occur as a result of the quantities of information stored electronically, the E.U. Directive seeks "to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data."\textsuperscript{43} Previous data protection regulations such as the Organisation for Economic Cooperation and Development (OECD) Guidelines\textsuperscript{44} and the Council of Europe Convention\textsuperscript{45} neither standardized national legislation nor provided adequate privacy protection.\textsuperscript{46} Consequently, the Directive attempts to accomplish these goals by delineating specific norms and harmonizing data protection laws throughout Member States.\textsuperscript{47}

B. Prior European Legislation

1. OECD Guidelines

On September 23, 1980, the OECD\textsuperscript{48} recommended the "Guidelines


\textsuperscript{43} The Convention for the Organisation for Economic Co-operation and Development is designed to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to

\textsuperscript{44} OECD Doc. C(80) 58 final (Oct. 1, 1980).


\textsuperscript{46} \textit{See PRIVACY AND DATA PROTECTION, \textit{supra} note 39, at 24.}

on the Protection of Privacy and Transborder Flows of Personal Data” to prevent the increasing threat to personal privacy in the collection of data. The Guidelines urge Member States to adopt data protection measures to ensure personal privacy, to avoid creating obstacles to transborder flows of personal data, and to agree on specific procedures for the application of the Guidelines. They outline basic principles for both data protection and the free flow of information among countries that have laws conforming with the protection principles. As of 1994, all OECD Member States have adopted the Guidelines.

The adoption of the OECD Guidelines does not eliminate threats to personal privacy in electronically stored data. The Guidelines provide a standard against which Member States can model their laws; however, the Guidelines themselves have no legal force. For the Guidelines to be effective, Member States must enact domestic laws that apply the OECD Guidelines; as a result, the Guidelines allow broad variation in national implementation. The OECD still monitors developments in this area and provides a forum for discussion on the issues arising in privacy and data protection; however, it has not created uniformity throughout the data protection laws in the different nations.
2. Council of Europe No. 108

One year after the OECD issued the Guidelines, the Council of Europe passed the "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." Concluded January 28, 1981 in Strasbourg, the Convention protects automated personal files in both the public and private sectors. The Council of Europe recognizes that while the free flow of information is necessary for transborder economic activities, there are inherent dangers from the introduction of electronic treatment of personal data in many sectors of private life. Thus, the Council of Europe implemented this Convention to ensure that an individual could practice his or her constitutional rights. In particular, the Convention requires proper safeguards for the treatment of sensitive data such as medical records, race, or religion.

The Convention is similar to the OECD Guidelines; however, the Council requires Member Countries to enact legislation conforming to the Convention to protect personal privacy. The Convention provided a framework for domestic legislation. However, like the OECD, the Convention did not standardize the data protection legislation throughout Member States.

C. E.U. Directive

The European Union attempted to define regulations for electronically stored personal data due to the "uneven application and great variation of national laws permitted by both the Guidelines and the Convention."

---

59 See GORE & BROWN, supra note 10, at 22 (stating that both the OECD and the Council of Europe privacy guidelines recognized that the importance of the free flow of information is critical to transborder economic activity).
61 Id.
62 Id.
63 See GORE & BROWN, supra note 10, at 22 (stating that the Council of Europe adopted "fair information practices" similar to those stated in the OECD regarding the regulation of collection, storage, and automated processing of personal data and transborder data flow).
64 See Cate, supra note 58, at 432.
65 See PRIVACY AND DATA PROTECTION, supra note 39, at 24.
66 Cate, supra note 58, at 432. See also Amended Proposal for a Council Directive
Beginning in 1990, and continuing through subsequent amendments,\(^6^7\) the Commission for European Communities (C.E.C.) released several proposals for the creation of Council Directives relating to data protection before the final passage of this Directive.\(^6^8\) The European Union recognized that data processing systems contribute to economic and social progress as well as trade expansion.\(^6^9\) The diverse approaches to data protection and the development of an internal market were obstacles to unhampered market expansion.\(^7^0\) The Directive attempts to protect an individual's personal privacy by both reconciling the varying degrees of data protection legislation and including data stored in private and public sectors.\(^7^1\) As such, the Directive requires that these systems also respect fundamental freedoms and rights of individuals such as the right to privacy.\(^7^2\)

1. The Directive Seeks to Narrow Differences Among State Laws

Through a slow and steady transition in the Member States themselves,\(^7^3\) the Directive seeks to narrow the differences among national data protection laws to encompass the rights of individuals throughout Europe.\(^7^4\) By requiring uniform regulations for the treatment of personal on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM (92) 422 final at 30 (the amended version was submitted by the Commission on Oct. 16, 1992).


\(^6^8\) PRIVACY AND DATA PROTECTION, supra note 39, at 24.


\(^7^0\) PRIVACY AND DATA PROTECTION, supra note 39, at 23.

\(^7^1\) See id.

\(^7^2\) See id.

\(^7^3\) The Member States have three years to implement the Directive. Council Directive, supra note 22, ¶ 69.

data, the Directive can ensure that the data traveling between countries receives equal treatment in each location. Once a Member State adopts the Directive, an individual has a right to privacy in the data processed about him or her, regardless of the Member State in which the processing occurs.\textsuperscript{75}

To secure an individual's right to privacy, the Directive restricts data transfer to non-Member states and creates common rules for businesses or administrations that collect, hold, or transmit personal data as part of their activities.\textsuperscript{76} Once a Member State adopts the Directive, these businesses and administrations can collect data only for specific and legitimate purposes.\textsuperscript{77} The businesses and administrations must ensure that all data is relevant, accurate, and up-to-date.\textsuperscript{78} If these businesses and administrations transfer data to non-Member countries, those countries receiving data must ensure that they will process the data with an adequate level of privacy protection.\textsuperscript{79} Consequently, a country who meets the E.U. Direct-

\textsuperscript{75} Council Directive, \textit{supra} note 22, art. 1 (stating that the right to privacy, one of the fundamental rights and freedoms, is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Union law). \textit{See New Rules, supra} note 74. Member States of the European Union will still maintain their national data protection laws. Council Directive, \textit{supra} note 22, art. 1 ¶ 1. These laws will provide for the treatment of data where the collection of such information is handled by an administration that is not established on E.U. territory or in an E.U. country, for example, a foreign government or a tax collection agency. These organizations are traditionally not subject to the laws of the Member State in which they operate; however, the Directive maintains that national laws will cover these organizations. \textit{New Rules, supra} note 74.

\textsuperscript{76} Council Directive, \textit{supra} note 22, arts. 6, 7. Article 6 of the Council Directive requires Member States to provide that personal data "must be (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes . . . . (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate . . . up to date . . . ." Article 7 provides further that Member States shall provide guidelines under which personal data can be processed such as where the "data subject has unambiguously given his consent," and processing is necessary for the performance of a contract to which the data subject is a party, processing is necessary to protect the vital interests of the data subject. \textit{Id.}

\textsuperscript{77} \textit{See New Rules, supra} note 74.

\textsuperscript{78} \textit{See id.}

\textsuperscript{79} \textit{Id.} The E.U. Directive does not define what level of protection is necessary for a third party country to receive data:

\textit{[t]he adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in}
tive's minimal level of data protection will be permitted to receive data from each of the sixteen Member States. This provision has particular implications for the United States. As the United States and the European Union are each others' largest trading partners, the United States is extremely dependent upon the free flow of information among nations. This E.U. Directive potentially eliminates data transfer between an European country and the United States, because the United States does not have comprehensive national data protection legislation to protect an individual's right to privacy.

2. Individual Rights under the Directive

In addition to specifying rules for the treatment of information, the Directive provides a "data subject" with certain rights, and requires specific treatment for classes of information it considers particularly sensitive. An individual has a right to access the data pertaining to himself or herself, know the source of the data, and correct misinformation. The Directive allows the individual to have legal recourse if such data is unlawfully processed. The Directive requires specific treatment for information pertaining to ethnicity or race, political beliefs, religious affiliation, trade union membership, and health or sexual life. This information can only be processed with the individual's consent. An individual has the option whether to provide information that will be stored in a database.

Although the Directive attempts to secure an individual's right to privacy, it exempts certain areas from regulation. The Directive does not regulate data pertaining to state security measures or personal data necessary for the economic well-being of the State. Furthermore, where data is collected by a third party, that third party is not required to notify the individuals whose data is being processed. Instead, the Directive

force in the third country in question and the professional rules and security measures which are complied with in that country.

Council Directive, supra note 22, art. 25 ¶ 2. Note, however, that the "Commission may find . . . that a third country ensures an adequate level of protection . . . by reason of its domestic law or of the international commitments it has entered into . . . for the protection of the private lives and basic freedoms and rights of individuals." Id.

See id.

Legislative Framework, supra note 6.

New Rules, supra note 74.

See id.

See id.

Legislative Framework, supra note 6.


The Directive states that where a "disproportionate effort" would occur, the
merely requires that all data processing have a proper legal basis. 88 The data collection is evaluated in light of the purpose for which it is collected. The legal grounds are "consent, contract, legal obligation, vital interest of the data subject, or the balance between legitimate interests of those controlling the data and those on whom the data is held." 89

The ambiguity of certain parts of the E.U. Directive highlights the difficulty in creating comprehensive and uniform data protection legislation throughout several countries. For example, the Directive permits data transfer among Member States as long as the states have equivalent data protection legislation. 90 Arguably, the legislation will be similar because each Member State's national laws must comply with the E.U. Directive. Yet, the equivalency of the national laws will be judged on a sector by sector basis. 91 This could lead to ad hoc and uneven application of data protection laws, a result the Directive sought to avoid.

3. Potential for Competitive Advantage

In addition to protecting an individual's right to privacy in the data collected about himself or herself, 92 the implementation of the Directive suggests that the European Union will use the Directive to form a competitive advantage over non-Member Countries. The Directive disallows transmitting data to non-Member Countries unless those counties have minimal levels of data protection. 93 Few states outside the European Union had data protection laws when the European Union initiated discussions regarding the creation of uniform data protection legislation among Member States. 94

Furthermore, implementation of data protection legislation promotes consumer confidence and allows for the development of the information society. 95 The lack of consumer confidence in the United States could be affected...
a barrier to growth, while the European Union has eliminated such barriers.

The Directive is also seen as a necessary measure to foster trade relations among countries. The lack of comprehensive data protection legislation among states in the international market is feared to be an impediment to continued market growth because countries could block the transfer of information among themselves. By standardizing legislation, the Member States can more freely transfer information and promote trade relations; participation by the United States could be hampered.

III. LORTAD: SPAIN'S DATA PROTECTION LAW

Spain, one of the E.U. Member States, recently enacted data protection legislation to regulate data stored by both the private and public sectors. Titled the "Law on the Regulation of the Automated Processing of Personal Data," (LORTAD) Spain's law is a reaction to technological advances that have resulted in large quantities of personal information being stored electronically. Article 18.4 of the Spanish Constitution already grants citizens a right to privacy in electronically stored data and attempts to limit access to such data; however, the Spanish Parliament recognized that constitutional protections alone would not protect an individual from unwarranted intrusions into personal data and meet the minimal standards of the E.U. Directive. Therefore, the Spanish Parliament enacted LORTAD to define protected areas and to continue and promote its participation in the world market. Spain's at-
tempt to legislate arguably already constitutionally protected areas, demonstrates that even if the United States could find a constitutional right to privacy in electronically stored information, that right is insufficient to protect and conform with the E.U. Directive.

A. The LORTAD and its Provisions

LORTAD’s objective “to limit the use of information technology and other techniques and means of automatic treatment of data of a personal nature, in order to guarantee the protection of the reputation, and the privacy of individuals and their families and the full exercise of their constitutional rights,” is carried out through the Data Protection Agency.103 At passage, LORTAD was merely a skeletal piece of legislation; the law specifies certain areas that warrant protection, but gives the Data Protection Agency the authority to promulgate specific regulations to promote conformance with the rules.104 Moreover, the Data Protection Agency, along with industry standards and national regulations, regulates the storage, transmission, and collection of data.105 The following discus-

different legal demands including Article 18.4 of the Spanish Constitution, the European Council Agreement 108, the E.E.C. Treaty, the Treaty of Maastricht, and the Schengen System of Information. Id.

103 Id. art. 1. Article 1 explicitly states LORTAD’s objective:

[[la presente Ley Orgánica, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.

Id. Translation to English by author unless otherwise noted. In Spain, privacy not only signifies the right to be left alone, but also is defined as “a spiritual internal zone reserved for a person, or a group, especially a family. MIGUEL CASTAÑO, DERECHO A LA INFORMACIÓN FRENTE AL DERECHO A LA INTIMIDAD: SU INCIDENCIA EN EL SISTEMA DE INFORMACIÓN ESTADÍSTICA 35-36 (1983).

104 As will be discussed more thoroughly below, one area of particular concern in Spain is data pertaining to an individual’s health records. As a result, the Data Protection Agency recently drafted a decree requiring financial institutions to destroy any health information concerning their clients within one month of the official publication of the decree. Banks often collect this information prior to processing loans or life insurance applications. See Spain Decrees Client Secrecy, 7 LIFE INS. INT’L, May 1, 1995, available in 1995 WL 14385778.

105 See id. For example, recently the Data Protection Agency, in accordance with LORTAD’s regulations pertaining to health and medical records, stated that banks will no longer be able to stock information on the health of their clients. This information is collected for insurance and loan grants. Once the decree is published, banks will have one month to destroy any health information pertaining to clients in their databases. See id.
sion highlights some of LORTAD’s provisions, explains LORTAD’s back-
ground, and demonstrates how Spain attempted to legislate in areas where
constitutional protections already existed.\textsuperscript{106}

Although Article 18.4 of the Spanish Constitution grants citizens a
right to privacy in electronically stored information, the Spanish Parlia-
ment enacted LORTAD to articulate the precise constitutional guarantees
each individual possesses in the present day information society.\textsuperscript{107}
LORTAD explicitly recognizes potential threats to an individual’s privacy
in light of increased technological advances in collection, storage, and
access to electronically stored data.\textsuperscript{108}

In attempting to protect an individual’s constitutional rights, the law
recognizes that data regulation should occur at each level of data handling
such as data collection, processing, storage, communication, modification,
usage and deletion, or ultimate disposal to prevent the misuse of personal
data and protect an individual’s right to privacy.\textsuperscript{109} The law governs
both the private and public sectors,\textsuperscript{110} and therefore places restrictions
on information transfer between companies.\textsuperscript{111}

1. The Spanish Constitution of 1978 and the Spanish Right to
Privacy

While numerous European countries have data protection legislation,
Spain’s legislation merits careful attention due to the historical backdrop
against which it was enacted. The current Spanish Constitution, the


\textsuperscript{107} Id. at Exposición de Motivos § 1. In pertinent part LORTAD states, “[l]a
Constitución española, en su artículo 18.4, emplaza al legislador a limitar el uso de la
informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos
y el legítimo ejercicio de sus derechos. La aún reciente aprobación de nuestra
Constitución y, por tanto, su moderno carácter, le permitió expresamente la articulación
de garantías contra la posible utilización torticera de ese fenómeno de la
contemporaneidad que es la informática.” Id.

\textsuperscript{108} See id. In pertinent part, the law states that “[e]l progresivo desarrollo de las
técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha
expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida.” Id.

\textsuperscript{109} Id. See also Ana Rosa González Murúa, El derecho a la intimidad, el derecho
da la autodeterminación informativa y la L.O. 5/1992, de 29 de octubre, de regulación
del tratamiento automatizada de datos personales, 96 WORKING PAPERS: INSTITUT DE

\textsuperscript{110} B.O.E., 1992, 262 art. 2.1.

\textsuperscript{111} Jo Anne Parke, The Case for Going Global, TARGET MARKETING, Nov. 1994, at
8; cf. infra Part IV discussing current U.S. legislation such as the Privacy Act of 1974
and the Freedom of Information Act, which only regulate data stored by the govern-
ment.
Constitution of 1978,\textsuperscript{112} states that Spanish citizens have a right to privacy.\textsuperscript{113} In addition to the general right to privacy annunciated in Article 18.1, the Constitution specifies particular areas where the state will safeguard an individual’s privacy, including religion and ideology.\textsuperscript{114} The Constitution further recognizes that numerous types of personal information are susceptible to privacy abuse, and therefore guarantees in Article 18.4 that “the law will limit the use of information technology in order to safeguard the honor and privacy of the person and the family of citizens and the full exercise of their rights.”\textsuperscript{115}

In creating Article 18.4, Spain recognized the dangers inherent in electronically stored information. Yet Spain’s enactment of LORTAD demonstrates that even a constitutional guarantee may be insufficient to protect this particular right to privacy. LORTAD recognizes that the citizens’ constitutional right—that the law will limit the use of electronically stored information of a personal character—may be insufficient to encompass the immense number of possible abuses.\textsuperscript{116} Prior to modern advances, an individual did not need an explicit constitutional provision or law to protect his privacy because the “frontiers of privacy were defended by time and space.”\textsuperscript{117} Time enabled an individual’s past events to disappear from record or memory, and space provided sufficient distance such that individuals in another location could not easily obtain information about one another.\textsuperscript{118} The constitutional right may not be broad enough to encompass the new frontier of privacy rights that have emerged from advances in modern technical communications.\textsuperscript{119} Com-

\textsuperscript{112} Depending upon how one counts the Spanish Constitution, this will be regarded as Constitution number ten or number thirteen. See George E. Glos, The New Spanish Constitution, Comments and Full Text, 7 HASTINGS CONST. L.Q. 47 (1979) (providing a detailed analysis of the Spanish Constitution of 1978).

\textsuperscript{113} Article 18.1 states, “[t]he right to honor, to privacy of the person and of the home, and to one’s likeness are guaranteed.” C.E. art. 18.1.

\textsuperscript{114} To determine what areas of one’s life and what specific details Spain intends to include within the constitutionally protected right to privacy, one only has to examine other constitutional provisions. For example, Article 16.2 of the Spanish Constitution states that “no one will be required to disclose his ideology, religion, or beliefs.” Id. art. 16.2.

\textsuperscript{115} Id. art. 18.4.

\textsuperscript{116} Ley Orgánica de 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, (B.O.E., 1992, 262), at Exposició de Motivos § 1.

\textsuperscript{117} Id.

\textsuperscript{118} Id.

\textsuperscript{119} Id. With technological advances, an individual can compile information about another and create a profile of that individual. Id.
puters have eliminated these protective devices. Therefore, an explicit law is necessary to define the limits of the use of information and the extent of individual privacy rights within this new electronic frontier.\(^{120}\)

The law is also necessary in areas even where Spain has already legislated. According to LORTAD, specific areas warrant express legislative protection.\(^{121}\) Among these areas are data concerning religion, ideology, or beliefs,\(^{122}\) and data concerning racial origin, health, or sexual life.\(^{123}\)

2. Alternative Motives behind LORTAD’s Implementation

According to the Spanish Parliament, Spain enacted LORTAD to extend the constitutional protection explicitly stated in the Constitution of 1978.\(^{124}\) However, Spain’s increasing participation in the global market and interactions with European nations, suggest that Spain created LORTAD not only to safeguard an individual’s right to privacy, but also to secure its position in the international market place. In 1985, a draft data protection bill was submitted to the Spanish Parliament. Yet no action was taken on this bill until 1990 when both the Council of Europe and the European Union began to apply pressure on Spain to adopt the bill.\(^{125}\)

Numerous European countries had data protection laws prior to Spain,\(^{126}\) and therefore Spain’s ability to actively participate in the European Union was contingent on its enactment of data protection legislation. Prior to LORTAD, other European nations would not transmit electronically stored data to Spain because Spain lacked a comprehensive law on

\(^{120}\) _Id._ ("The fixation of this new frontier is the object of the provision contained in Article 18.4 of the Constitution, and the present law compliments this objective.").

\(^{121}\) _Id._ art. 7.

\(^{122}\) _Id._ art. 7.2 (stating that data pertaining to this type of information is protected in accordance with Article 16.2 of the Spanish Constitution).

\(^{123}\) _Id._ art. 7.3; art. 8. Article 8 pertaining to health is particularly noteworthy because Spain already has legislation protecting the privacy of an individual’s health record.

\(^{124}\) _Id._ (stating that the law will articulate constitutional guarantees of Article 18).

See also González Murúa, _supra_ note 109, at 4.

\(^{125}\) See Madsen, _supra_ note 3, at 63.

\(^{126}\) For example, both the United Kingdom and France have comprehensive and extremely detailed data protection laws. The United Kingdom’s law, the Data Protection Act of 1984, provides a framework for finding a balance between interests of the individual, data user, and the community. France’s law, the Data Protection Act, encompasses data collected in both the public and the private sector. For a detailed study of the data protection legislation throughout the world, see Madsen, _supra_ note 3, at 998.
data protection.\textsuperscript{127} As a result, LORTAD sought to incorporate several international agreements to prevent further international restrictions on data transfer.\textsuperscript{128} Furthermore, as early as 1981, organizations and companies expressed concern about the risks of using automatically treated information.\textsuperscript{129}

Prior to enacting LORTAD, Spain passed several laws expanding and clarifying an individual's constitutional rights. In 1982, in accordance with the rights to honor and intimacy under Article 18 of the Spanish Constitution,\textsuperscript{130} the Spanish Parliament passed the law for the "Civil Protection of the Right of Honor and Personal Intimacy."\textsuperscript{131} The regulation codified specific violations, and demonstrated its intent: to protect the individual's rights of honor and personal intimacy as much as possible. It was not until several years later, however, that the increase in technological advances forced Spain to consider codifying Article 18.4. In 1982, Spain reorganized information services within the Sistema de Informatica Fiscal Distribuida (SIFD).\textsuperscript{132} This reorganization resulted in new database techniques on the national, regional, and provincial levels.\textsuperscript{133} The new computerized system enabled those individuals with access to the personal information stored within to manipulate the data. Spain recognized the enormous impact the reorganization could have, and therefore attempted to maintain confidentiality regarding the data and its use.\textsuperscript{134} The resulting law requiring confidentiality in the reorganized system was the beginning of a series of attempts to determine the extent of an individual's rights under Article 18.4 of the Spanish Constitution.

C. Competing Interests in the Spanish Constitution

Data protection in Spain refers to the legal protection individuals realize in the treatment of their personal data.\textsuperscript{135} In addition to guaranteeing the right to privacy in Article 20.1, the Constitution also guarantees the right "to freely express and disseminate one's thoughts, ideas and

\textsuperscript{127} See id. at 63.
\textsuperscript{128} See supra note 116 and accompanying text.
\textsuperscript{129} CASTAÑO, supra note 103, at 41.
\textsuperscript{130} C.E. art. 18.1.
\textsuperscript{131} Civil Protection of the Right of Honor and Personal Intimacy (B.O.E., 1982, 115).
\textsuperscript{132} Sistema de Informatica Fiscal Distribuida (B.O.E., 1982, 190). The information stored in these databases pertained mostly to economics and police records. Id.
\textsuperscript{133} Id.
\textsuperscript{134} Id.
\textsuperscript{135} DERECHO INFORMATICO, supra note 1, at 49.
opinions by speech, writing, or any other means of reproduction." This article expands this freedom to include the right "to freely transmit and receive true information by any means of broadcasting." It is not the data itself that necessitates constitutional protection, but instead the character of the data allowing personal information to be disseminated. This information can affect an individual, and in doing so infringe on his or her constitutional rights of privacy and dignity. Thus, the constitution guarantees both access to information and the right to privacy. Data protection legislation sought to strike a balance between these two competing interests.

To accomplish the balance between the right to privacy and the right to information, LORTAD first recognized and then defined the parameters for each right. Article 13 of LORTAD recognizes that individuals have the right to information, and therefore allows interested parties to request information about others from the General Registry. This right, however, still protects an individual's constitutional rights to privacy and dignity because it limits dissemination to particular categories of information. Furthermore, the individual about whom the data is stored has a right to inspect and have access to his or her data. These rights thus grant individuals other than the affected individual access, while providing the affected individual with constitutional guarantees of privacy.

Several of LORTAD's articles are subject to constitutional attack and arguably infringe on an individual's right to privacy. LORTAD includes a consent provision that requires the affected individual to consent to the gathering of his or her personal data. The individual must have

---

134 C.E. art. 20.1(a).
135 Id. art. 20.1(d).
137 C.E. art. 16. Individuals have a constitutional right to privacy regarding their religion and ideology. Id. This information will not be disseminated. B.O.E., 1992, 262.
138 González Murúa, supra note 109, at 8.
139 B.O.E., 1992, 262.
full knowledge of what will become of his or her personal data. The law thus appears to protect an individual’s right to privacy; however, Article 5 of LORTAD exempts this consent provision in particular circumstances and establishes an individual’s right to access information.\footnote{Id. art. 5. Affected parties must be informed of the following: (a) the existences of an automatic or computerized file of the data of a personal nature, the purpose for which the information is gathered and the recipients of the information; (b) whether it is obligatory or optional to reply to the questions put to them; (c) consequences of data being gathered or the consequences of refusing to supply the data; (d) possibility of exercising the rights of access, correction and deletion; and (e) identity and address of party in charge of the file. Id.} The numerous exceptions to the consent provision include: data obtained from sources readily accessible to the public such as commercial or real estate registers or telephone directories, or data referring to individuals linked by business, labor, or administrative relations or by a contract.\footnote{See Rodriguez, supra note 100. In recent years Spain has become an attractive market for foreign investment. During the late 1960s and early 1970s, economic growth occurred in Spain at a rate above other European countries. As a result, a new middle class emerged to access the level of consumption present in fully developed countries. Spain’s attractiveness in the international market increased significantly during the 1980s when Spain joined the European Union. See id.} While there may be constitutional challenges to the law, LORTAD’s framework demonstrates the attempt to balance the right to privacy with the right to access of information. The Data Protection Agency can further assist in defining the law as later challenges arise.

D. Other Concerns Prior to Enacting LORTAD

During the 1980s, Spain became an attractive market for international business.\footnote{See id.} The direct marketing industry in particular, realized incredible growth.\footnote{See id.} This industry, however, is perhaps most significantly affected by LORTAD. Although the Spanish Parliament passed LORTAD to safeguard an individual’s right to privacy and not specifically to regulate the direct marketing industry, the regulation left most of the industry illegal.\footnote{See id.} The direct marketing industry gained substantial sums from selling information in the form of customer lists and from catalogue sales. LORTAD prohibited those engaged in the direct marketing industry from selling lists containing consumer information to other agencies. Contrary to expectations,\footnote{Spain-Direct Marketing Profile, Market Reports, Sept. 20, 1992, available in LEXIS, World Library, Allwld File (stating that specialists believe that LORTAD will}
lists and direct marketing, mail-order benefitted from the regulations and realized significant economic gains particularly from catalogue sales.\textsuperscript{151} Direct marketing analysts attribute this growth to the increase in consumer confidence in the industry.\textsuperscript{152} Thus, the success of this industry demonstrates that data protection laws can affect an individual's habits, and can actually aid the prosperity of an industry.

IV. DATA PROTECTION IN THE UNITED STATES

Although the United States is not immune from harms that result from the misuse of electronically stored information, it has not created comprehensive national data protection legislation. Instead, the United States responds to privacy concerns and harms that occur as a result of electronically stored information by passing sectoral legislation, legislation that only addresses the area of particular concern.\textsuperscript{153} In addition, in the public sector the United States responded to privacy concerns by passing both the Freedom of Information Act\textsuperscript{154} and its companion legislation, Privacy Act of 1974.\textsuperscript{155} As neither of these Acts nor legislation aimed at preventing abuses in particular sectors protect an individual’s right to privacy,\textsuperscript{156} the United States should enact comprehensive data protection legislation. The current state of U.S. legislation is unlikely to meet the minimum standard requirements of the E.U. Directive.\textsuperscript{157} Consequently,

\textsuperscript{151} See The Mail Order Market in Spain, National Trade Data Bank: Market Reports, March 21, 1995, available in LEXIS, World Library, Allwld File (explaining that the law helped companies because it stated how far the company could go toward collecting data; in addition, these new lists can be sold internationally, a practice that was previously restricted by an E.U. Directive); see also Rodriguez, supra note 100.

\textsuperscript{152} See Rodriguez, supra note 100.

\textsuperscript{153} See Joel R. Reidenberg, Data Protection Law and the European Union’s Directive: The Challenge for the United States: Setting Standards for Fair Information Practice in the U.S. Private Sector, 80 IOWA L. REV. 497, 499 (1995). The driving force behind such narrow fair information practice standards is the philosophy that government should be limited and that a "marketplace of ideas" allows only minimal restrictions on flows of information, including personal information. In a democratic society, “an individual’s desire for seclusion from the public realm opposes the societal value in a free flow of information for economic or political gain.” Id. at 500.


\textsuperscript{155} The Privacy Act of 1974 responded in part to concerns about the quantity of information stored by the government. For example, both police stations and intelligence agencies maintained numerous personal record systems. 5 U.S.C. § 552a (1974).

\textsuperscript{156} See supra notes 19-20 and accompanying text.

\textsuperscript{157} Council Directive, supra note 22, art. 25 ¶¶ 1, 4. Chapter IV of the Directive encompasses the regulations regarding the transfer of personal data to third countries. The specific regulations are set forth in Article 25:
E.U. Member States can prevent the transfer of data to the United States. This data is important for continued American success in the world market. The United States should examine LORTAD when creating its own legislation because Spain's law sought to balance the right to privacy with the right to access information where it incorporate areas of particular concern and meets the minimum requirements necessary to comply with the E.U. Directive. By creating data protection legislation that safeguards an individual's right to privacy, the United States could meet the requirements for transborder data flows from E.U. Member States to third party countries and consequently preserve its ability to receive data and actively participate in the world economy.

A. Right to Privacy in the United States and the Limits of the Constitution in Protecting Privacy in Electronically Stored Information

The U.S. Constitution, unlike that of Spain, does not explicitly guarantee an individual's right to privacy. Nonetheless, a right to privacy has evolved through judicial interpretation and legislative action. This right is not clearly delineated and its boundaries are continually tested; therefore, citizens need additional legislation to prevent their privacy from being invaded. In 1890, the future Justice Brandeis declared that privacy is the "right to be let alone," thus freeing the "privacy concept from its propertied and criminal procedure history."

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

4. Where the Commission finds . . . that a third country does not ensure an adequate level of protection . . . , Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

**Id.**

158 See supra note 31. Although the necessary level of data protection is ambiguous, the United States should not assume that E.U. Member States will continue to trade with the United States even though they are a large trading partner.

159 See, e.g., Griswold v. Connecticut, 381 U.S. 479 (1965) (recognizing a right to privacy in family matters such as birth control). See also Privacy Act of 1974 recognizing that a "right to privacy is a personal and fundamental right protected by the Constitution of the United States . . . ." 5 U.S.C. § 552(a).

160 See Jed Rubenfeld, The Right of Privacy, 102 HARV. L. REV. 737, 737 (1989) (stating that the right to privacy defines limits of governmental power, and "may on certain occasions render intolerable a law that violates no express constitutional guarantee").


162 C. Herman Pritchett, Forward to DAVID M. O'BRIEN, PRIVACY, LAW AND
phrase has echoed throughout case history and legislative interpretation to apply the right of privacy to a number of issues. Recognizing a "right to privacy" first occurred in constitutional terms nearly seventy-five years later in the Supreme Court's decision in *Griswold v. Connecticut,* the constitutional source of this right remained ambiguous. Subsequent decisions illustrate that the Court can find a right to privacy "in the penumbras of the Bill of Rights," and in the concept of liberty guaranteed by the due process clause of the Fourteenth Amendment. Furthermore, several states have amended their constitutions to ensure an individual's right to privacy. Case law and statutes alone, however, have not eliminated intrusions into an individual's privacy, nor have they clearly delineated what areas are constitutionally protected.

PUBLIC POLICY at vii (1979). The 1890 Brandeis and Warren article expanded the privacy context beyond the Fourth Amendment, which subjected searches and seizures to warrant requirements, and the Fifth Amendment which placed a ban on self-incrimination. The 1886 Supreme Court decision of *Boyd v. United States* initiated a broad interpretation of the Fourth and Fifth amendments in the context of criminal prosecutions. *Id.*

163 See *id.* For example, the collection of personal information in computers and data banks that make complete life histories available to individuals with access to computer terminals. *Id.*

164 381 U.S. at 479 (overturning a state statute making it a criminal offense either to use birth control or to give information or instruction about its use because the statute unconstitutionally infringed upon a fundamental right of privacy in the marriage relationship).

165 *Id.* Justice Douglas found a right to privacy in the "penumbras" of the First, Third, Fourth, Fifth, and Ninth Amendments, while two other justices found a right to privacy in the due process clause of the Fourteenth Amendment. *Id.*

166 *Id.*


168 See, e.g., ARIZ. CONST. art. II, § 8 ("Right to Privacy. No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); R.I. GEN. LAWS § 9-1-28.1 (1980) ("It is the policy of this state that every person in this state shall have a right to privacy."). Other states with some form of privacy protection include Georgia, Virginia, and Washington.

169 See Rubenfeld, supra note 160, at 740. This right to privacy is distinct from that expectation of privacy secured by the Fourth Amendment. See *id.* Rubenfeld argues that privacy in this context governs the conduct of those who intrude upon others' lives. For privacy can be understood "in its familiar informational sense; it limits the ability of others to gain, disseminate, or use information about oneself. By contrast, the right to privacy that concerns use attaches to the rightholder's own actions." *Id.* Both these ideas concerning an individual's right to privacy are embodied in the right to privacy in the data stored about oneself.
Although several constitutional amendments, in particular the Fourth Amendment, suggest a right to privacy in electronically stored information, this right has not been protected as if it were implicit in the fundamental right to privacy. The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures . . . .". Yet individuals, businesses, and governments have all been subjected to violations because of invasions into various databases. Intrusions into a database can disclose characteristics about an individual and in turn define who the person is. Thus, access can threaten the overall concept of life and liberty of the person and the right to be secure in his home.

As intrusions into one's life threaten the concept of liberty, recognizing a right to be free from unwarranted invasions into one's life through electronically stored information appears to be merely an extension of the rights guaranteed in the Fourth Amendment. The Fourth Amendment grants individuals protection against unreasonable searches and seizures of houses, persons, and effects; however, electronically stored information is not necessarily present in one location such that the Fourth Amendment can provide sufficient protection. The constitutional protection, however, is troublesome because of the location of the information. As such, the Fourth Amendment alone will not provide an individual with sufficient privacy protection. Once an individual provides information that ultimately becomes part of a database, the individual no longer has possession of that information. Intrusions into the individual's privacy do not occur within that individual's home, or other areas that are constitutionally protected by the Fourth Amendment. Consequently, the application of

---

170 U.S. CONST. amend. IV.
171 These abuses occur due to unwarranted intrusions, carelessness, or the plain error of data handlers. See, e.g., Ann Merrill, Privacy for Sale, STAR TRIB., Feb. 11, 1996, at 1D (discussing how a data handler's error affected nearly one-half of a small town's residents). In Norwich, Vermont, nearly half of the town's 3,500 residents were unable to obtain loans, mortgages, or credit cards due to an error made by an employee of the credit bureau Equifax. The town council became involved and attempted to remedy the situation. The credit bureau did not act to correct the errors until a Wall Street Journal article exposed the problems. Id. See also Michael W. Miller, Equifax Says Credit Reports Had Mistake, WALL ST. J., Mar. 30, 1992, at C16 (discussing the Norwich situation).
172 See Today Show: Private Lives (NBC television broadcast, Feb. 26, 1996), available in 1996 WL 3699428 (discussing privacy abuses that can occur when information is obtained and manipulated). This information can be used to manipulate an individual's records and cause numerous problems. For example, a Houston couple, Sandy and Bill Dwyer, became the victims of fraud when someone accessed their credit records from a car dealership in Florida. That individual used the information to apply
the Fourth Amendment to electronically stored data is problematic in part because of the inability to pinpoint the location where another person intercepted and misused the data as well as the failure of the invasion to occur in the home. Instead, the United States needs to create comprehensive legislation to delineate the limitations of a constitutional right to privacy, and to legislate in areas where the Constitution may be unable to afford sufficient protection.

B. Access to Information and the Right to Privacy

In addition to an individual’s right to privacy, legislative action in the United States demonstrates that individuals have a right to access information. The Freedom of Information Act provides individuals with access to all government agency records unless specifically exempted. The Privacy Act of 1974, the companion legislation to the Freedom of Information Act, attempts to provide safeguards for an individual against invasions of personal privacy. Ability of individuals with

for, and ultimately obtain, credit card accounts which in turn were charged with over $20,000. It took the Dwyers over two years to clear their name and regain their identity because they could not convince the credit card companies that they did not make the questionable purchases or open the accounts. See Today Show: Part 2-Private Lives (NBC television broadcast, Feb. 27, 1996), available in 1996 WL 3699462. The Dwyers’ story is not unique. In fact, individuals throughout the world can become victims of abuse. Individuals with good credit ratings are particularly suspect. See also R.J. Ignelzi, Privacy, Identity, Theft, SAN DIEGO UNION-TRIB., July 2, 1995, at D1 (discussing the story of a forty-five year old woman who became the victim of credit card abuse). These incidents, known as “personal identity theft” occur when someone takes the personal information of another to create a false persona for fraudulent purposes. Lawyers and specialists estimate that this type of fraud is growing by 34% per year. Id.

Premised upon traditional notions of self-regulation and discourse, the FOIA provides individuals with the ability to access data. Although FOIA discussions inevitably focus on what may be withheld, “disclosure, not secrecy, is the dominant objective of the Act.” Department of the Air Force v. Rose, 425 U.S. 352, 361 (1976). The Act establishes requirements for disclosure by publication in the Federal Register; availability for public inspection and copying; or release pursuant to a request for access from “any person.” LITIGATION UNDER THE FEDERAL FOIA AND PRIVACY ACT 1 (Allan Adler ed., 15th ed. 1990) (hereinafter LITIGATION UNDER THE FOIA). There are seven specific exemptions to the FOIA, see infra note 184.


The Act sought to “safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes.” 5 U.S.C. § 552a. The Privacy Act was originally designed to
access to computers to gather personal information about others threatened the already tenuous right to privacy and led Congress and most states to pass legislation protecting privacy in broad terms. The Privacy Act attempts to guard citizens from the misuse of personal data gathered and stored in federal information banks. The Privacy Act enables individuals to obtain their personal records stored by federal agencies, and dictates that those agencies only retain information relevant to a specific and legal purpose. The reach of the Privacy Act is extremely limited; however, because it only concerns information stored by the public sector.

C. Past Legislative Failures and Individual Skepticism

At present, the United States does not have comprehensive data protection legislation. The Freedom of Information Act and the Privacy Act of 1974 have been largely ineffective in securing an individual’s right to privacy in electronically stored information and finding an appropriate balance between access to information and a right to privacy. These prevent the Federal government from invading an individual’s privacy; at that time, the use of computers by the government was rapidly expanding. Id.

Section 2 of the Privacy Act of 1974 recognized the potential abuses inherent in storing large amounts of personal information. In pertinent part it states:

1. the privacy of an individual is directly affected by the collection, maintenance, use and dissemination of personal information by Federal agencies;

2. the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information;

3. the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems . . . .


Pritchett, supra note 162, at vii. For example, in 1974, the same year that Congress passed the Federal Privacy Act, California adopted a constitutional amendment stating: “all people are by nature free and independent, and have certain inalienable rights, among which are those of enjoying and defending life and liberty; acquiring, possessing, and protecting property; and pursuing and obtaining safety, and happiness and privacy.” Id.


Id.

As a result of the Privacy Act, a Privacy Protection Study Commission received a congressional mandate to investigate the personal data handling practices within both the government and the private sector. It was this commission that recommended that the Act not be extended to cover the private sector. MADSEN, supra note 3, at 107.

The highly publicized hostage situation of Terry Anderson illustrates the failure
Acts also fail to provide privacy protection because of the uneven application of the regulations for information requests. According to the Privacy Act of 1974, individuals can obtain information about themselves stored in federal data banks.\(^{182}\) Release of information under either of these Acts requires a balancing test that does not always result in uniform application.\(^{183}\) The Freedom of Information Act contains specific exemptions that restrict the dissemination of information.\(^{184}\) Of particular im-

---

\(^{182}\) FOIA, 5 U.S.C. § 552.

\(^{183}\) See generally LITIGATION UNDER THE FOIA, supra note 173, at 115-35.

\(^{184}\) FOIA, 5 U.S.C. § 552(b)(1)-(7). The Freedom of Information Act states that the provisions relating to the disclosure of information do not apply "to matters that are—

(1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by statute (other than section 552b of this title) provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to fair trial or impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy; (D) could reasonably be expected to disclose . . . confidential source . . . and, in the case of a record or information compiled by criminal law enforcement authority . . . information furnished by confidential source, (E) would disclose techniques . . . procedures . . . or guidelines for law enforcement investigations, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(8) contained in or related to examination, operating, or condition reports prepared by . . . for the use of agency responsible for the regulation or supervision of financial institutions; or

(9) geological or geophysical information and data, including maps concerning wells.
 importance to data protection legislation, and perhaps the most ambiguous, are Exemptions 6 and 7. According to Exemption 6, disclosure is prohibited where "it would constitute a clearly unwarranted invasion of personal privacy." In such situations, government agencies can withhold distributing information stored in government files. Exemption 7 further prohibits the dissemination of information compiled for law enforcement purposes.

The Supreme Court attempted to clarify the ambiguities of the Privacy Act of 1974 and Exemptions 6 and 7 of the Freedom of Information Act regarding personal information in United States Department of Justice v. Reporters Committee for Freedom of the Press. In Reporters Committee, a CBS news correspondent and the Reporters Committee for Freedom of the Press filed suit to obtain FBI records known as "rap sheets" on Charles Medico. The FBI refused to release the information after a FOIA request had been made, and the suit followed. This decision illustrates the challenges that computerized databases present for balancing dissemination of information in accordance with these two Acts. The Court recognized that there is a difference between public records "that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information." The Court balanced the public interest in disclosure with Congress’ intent to determine whether access to information will be granted. The Court denied the press access to this information, stating that disclosure to a third party "could reasonably be expected to constitute an unwarranted invasion of personal privacy under" Exemption 7(C).

---

188 "Rap sheets" contain information about particular individuals compiled by the FBI. This information could include financial data and criminal history. 489 U.S. at 751-52.
189 Judge Starr, dissenting in the Court of Appeals opinion, stated that computerized data banks present issues different from a case involving source records themselves due to numerous state laws requiring cumulative, indexed criminal history information be kept confidential, as well as by Congressional indications about privacy and computerized databases. 831 F.2d 1128 (D.C. Cir. 1987).
190 489 U.S. at 764.
191 Id. at 776.
192 Id. at 771.
The Court further stated that it would use the balancing test for subsequent challenges.\textsuperscript{193}

In large part these Acts were unsuccessful because they did not reach data stored in the private sector. Although the release of information and the protection of privacy are not consistently measured under an uniform standard, the recent decision in \textit{Reporters Committee} could lead to a more uniform application of the statutes. This decision, recognizing that there are differences between electronically stored compilations and other forms of publicly stored information, could assist in the creation of a standard to protect an individual’s privacy in data stored by the private sector. The storage of information by the private sector is continually increasing.\textsuperscript{194} Without regulations on information stored by the private sector, affected individuals have little recourse and control over the course and dissemination of their personal information.\textsuperscript{195} Consequently, individuals suffer from disastrous results, often prior to their knowledge that anyone has stored information about them.\textsuperscript{196}

These Acts are also unable to protect an individual because they cannot control the misuse and abuse of data in federal data banks. Even though these Acts specifically regulate information stored by the federal sector, they are unable to control the vast quantity of information. Once an individual determines that his or her data has been misused, it is often difficult to determine the origin of the problem.\textsuperscript{197} Once the origin is determined, the penalties are not sufficient to deter future abuses.\textsuperscript{198}

\textsuperscript{193} \textit{See id.}

\textsuperscript{194} GORE \& BROWN, \textit{supra} note 10, at 21.

\textsuperscript{195} \textit{See, e.g.,} Guidmond v. Trans Union Credit Info. Co., 45 F.3d 1329 (9th Cir. 1995). Several individuals have been unable to adequately obtain compensation for errors that occurred in credit records. During the 1960s, the U.S. Congress passed the Fair Credit Reporting Act of 1988, 15 U.S.C. § 1681 (1988), in response to concerns over abusive credit reporting practices. Yet, numerous abuses in the credit card industry still result from the mass storage of information. In \textit{Guidmond}, the plaintiff alleged that Trans Union failed to correct incorrect information on her credit report despite her requests to do so. Guidmond alleged several violations under the FCRA. \textit{Id.}

\textsuperscript{196} \textit{See supra} note 171.

\textsuperscript{197} \textit{See} Michael R. Graham, \textit{ACLU: Officers Misuse Data: the State Organization’s Top Official Says Tighter Rules are Needed to Keep Officials from Abusing Computer Access for Personal Gain}, TUCSON CITIZEN, Sept. 4, 1995, at 1A. In September 1995, a Tucson police chief ordered an investigation of a high-ranking officer who had allegedly released computerized information about a criminal case to the media. Investigations are underway to determine the accuracy of these allegations and the source of the media leak. \textit{Id.}

\textsuperscript{198} \textit{Id.} For example, an eighteen-year veteran of the police force was accused of running the license plate numbers of women to determine their addresses. The officer then
Individuals use the information for personal gain, either monetary, social, or otherwise. Information abused by public officials or others utilizing data stored by federal or state data banks is particularly problematic because the police and other public officials are not required to release the electronically stored information.

Besides the Privacy Act of 1974 and the Freedom of Information Act, the United States legislated in certain areas as abuses arose to protect an individual's right to privacy. These Acts, however, do not amount to comprehensive legislation. Instead, of preventing abuses, they respond to abuses as they occur, and do not create sufficient remedies for affected individuals. For example, an individual may be aware that his or her credit report is inaccurate. If that individual has been harmed by this faulty rating, he or she must determine the appropriate statute under which to sue, and he or she must determine what type of error has occurred within a specified period of time. Placing such limitations on individuals retard their remedies because they are not knowledgeable about the proper course of action necessary to correct the wrongs. Furthermore, many intrusions simply are not challenged because people do not have enough money, or because an individual cannot protect his or her rights for personal reasons.

sent the women letters and asked for dates. The agent lost his job; however, his sentence was only fifty hours of community service and a $25 fine. Id.

199 Id. (stating that there are several documented cases of police officers using computers to obtain personal information about members of the opposite sex).

200 Id.

201 See supra notes 19-20.

202 For example, the Fair Credit Reporting Act, leaves several "grey areas." The three major credit bureaus — TRW, Trans Union Corporation, and Equifax — still can transmit an individual's personal information. While these organizations cannot divulge specific data about a consumer's financial information, they can use the data to group consumers into categories regarding their spending power. Michael Miller, Hot Lists: Data Mills Delve Deep to Find Information about U.S. Consumers, WALL ST. J. Eur., Mar. 15, 1991, at 1. Because these lists are not illegal, a consumer hurt by them (such as not obtaining a job) does not necessarily have any recourse against the company. See supra Part I, citing examples of sectoral legislation passed in the United States. See also Wayne Madsen, Clinton Proposes a Patchwork Approach to Data Protection, COMPUTER FRAUD & SEC. BULL., Nov. 1, 1993, available in 1993 WL 2577047 [hereinafter Madsen, Clinton Proposes a Patchwork Approach]. Madsen notes that the Computer Security Act of 1987, which established a Computer System Security and Privacy Advisory Board, has paid little attention to individual privacy protection in data. See id.

203 See Miller, supra note 202.
1. Congressional Attempts to Create Legislation

Despite the introduction of several bills before Congress, the United States has been unable to pass comprehensive data protection legislation. Recently, Representative Cardiss Collins\textsuperscript{204} introduced the Individual Privacy Protection Act of 1995.\textsuperscript{205} This bill would amend the privacy provisions of Title 5 to improve an individual’s privacy protection and create a permanent Privacy Protection Commission.\textsuperscript{206} It would enable private citizens greater recourse against the federal government.\textsuperscript{207} According to the proposed legislation, the Individual Privacy Protection Board would study data banks, data processing programs, and information systems of both public and private organizations.\textsuperscript{208} The Board would serve as a recommendation committee to determine standards and procedures as well as develop guidelines for the maintenance of individual records.\textsuperscript{209} This bill would comment on existing federal law, regulations, directives, and judicial decisions, and report on their consistency with the right to privacy and other constitutional guarantees.\textsuperscript{210}

In addition to the several attempts by Representative Collins to create a Data Protection Commission, another bill, entitled the Data Protection Bill of 1991, also proposed the creation of a permanent independent board to oversee data storage and data collection.\textsuperscript{211} This board would have focused on complaints, investigations, and reform in data protection.\textsuperscript{212} It was initially intended to provide a “focal point in a system

\textsuperscript{204} Representative Collins is a Democrat from Illinois.


\textsuperscript{206} Id. In pertinent part, H.R. 184 intends “to improve the protection of individual information and to reestablish a permanent Privacy Protection Commission as an independent entity in the Federal Government, and for other purposes.” H.R. 184, 104th Cong. (1995).

\textsuperscript{207} Id. The act would increase the amount of civil damages against the United States when an agency fails to maintain a record on an individual with accuracy, relevance, timeliness, or completeness to assure fairness, and it would also set limits on such recoveries. Id.

\textsuperscript{208} Id.

\textsuperscript{209} Id.

\textsuperscript{210} Id.


\textsuperscript{212} Id.
which operates without a permanent central structure." In contrast to Representative Collins' proposal, this bill would have focused solely on the creation of a data protection board. However, the bill was not enacted. Various senators have also introduced data protection legislation. But like the bills introduced in the House, the Senate bills never went to the floor for a vote.

Proposals for the creation of a data protection commission have also been introduced as amendments to existing legislation. In 1993, proposals were made to amend the Fair Credit Reporting Act to include a data protection commission. While several amendments to the Act became law, the data protection commission was not included in the final version. The concept of creating data protection legislation in the United States will likely continue to be part of the presented Congressional bills. Perhaps now that concerns are economic in light of the E.U. Directive, and not solely directed at protecting an individual's right to privacy, legislators will be more successful.

2. Support for U.S. Data Protection Legislation

The inability of Congress to pass comprehensive data protection legislation does not represent public opinion regarding data protection. Despite these traditional ideals of self-regulation and freedom from governmental control, popular support for data protection laws exists in certain areas. A recent Equifax survey illustrates that nearly four out of five Americans are concerned about threats to their personal privacy, and that the majority of Americans favor the establishment of a non-
DATA PROTECTION LEGISLATION

regulatory privacy board. Of particular importance is the creation of data protection legislation in the medical arena. If the United States created data protection legislation to protect an individual from unwarranted intrusions into medical data, they would be merely adding another piece of legislation; but it would not obtain a comprehensive data protection initiative. Instead of attacking a particular sector, the United States should follow Spain's lead and incorporate the varied data protection legislation into one comprehensive bill with special emphasis given to problematic areas.

In addition to public opinion regarding personal privacy in electronically stored data, the present administration, in particular, Vice President Albert Gore Jr., supports changes regarding international privacy principles. Gore advocates the following principles: collecting personal data for specified, legitimate purposes; disseminating, sharing, and reusing information compatible with the purposes for which it was originally collected; ensuring that personal data is accurate, relevant, and up-to-date; informing individuals where data will be used; allowing individuals to correct data; and transmitting personal data only when it is not "unduly restricted or subject to burdensome authorization procedures." Gore states that to accomplish the earlier goals, the United States should join other governments to identify key privacy issues and work with both the private and the public sectors to achieve fair information practices, while not allowing privacy protection to "impede the free flow of information across national borders." Furthermore, Gore advocates the use of voluntary guidelines such as those developed by the OECD. Unfortunately, relying on these Guidelines is insufficient for the United States to qualify as having adequate data protection legislation under the E.U. Directive. Despite Gore's statements, the Clinton administration has also stated that sectoral legislation is appropriate to protect an individual's privacy, and therefore, comprehensive data protection legislation is not necessary.

---

219 See id.
221 GORE & BROWN, supra note 10, at 22.
222 Id.
223 Id. at 22-23.
224 Id. at 23.
226 See Madsen, Clinton Proposes a Patchwork Approach, supra note 202 (discussing Clinton's proposals for three privacy panels: two to oversee the National Health Plan and one called for in the national health plan). Although the National Health Plan was not implemented, and hence these specific panels not created, if created, these panels...

Data protection legislation has the potential to curb industry both nationally and internationally. In particular, the direct marketing industry relies on customer lists and other information obtained from electronic databases. Several international businesses, particularly in the service sector (such as banks) also rely on the distribution of information. These areas, however, will not be harmed by the creation of data protection legislation. In fact, as Spain’s growth of the direct marketing and catalogue sales industry demonstrates, it is possible for the concerns to be wholly unfounded and for the United States to recognize significant growth in these areas.

As previously mentioned, the United States may be precluded from receiving data from E.U. Member States if it does not enact adequate data protection legislation.\(^\text{227}\) Some businesses, in particular service industries such as banking-related companies, have already been precluded from receiving information.\(^\text{228}\) As a result, these U.S. businesses compiled with the restrictions of other countries to continue the flow of data.\(^\text{229}\) In doing so, the U.S. banks did not suffer from any harm,\(^\text{230}\) thus demonstrating that perhaps U.S. industries overstate the potential harms.

Certain industries, notably the direct marketing industries, rely on the transfer of information, and are accustomed to buying and selling personal data files.\(^\text{231}\) Businesses that rely on direct marketing can be successful because they know the customer base to target.\(^\text{232}\) Thus, it is a lucrative business for both the compilers and sellers of lists as well as for the

\(^{228}\) See Ratcliffe & Waltz, supra note 32 (stating that U.S. businesses were restricted from receiving and transmitting information to German companies unless the United States complied with their laws).
\(^{229}\) See id.
\(^{230}\) See id.
\(^{231}\) See id. (stating that companies purchase medical, credit, and demographic information). See also Miller, supra note 202 (discussing different attempts to capitalize on the amount of information in the public sector). One company, Lotus Development Group, attracted attention to itself, when it announced plans to sell “Marketplace” a set of personal computer disks that contained data on nearly 120 million households. Lotus received numerous complaints, and as a result did not market the product.
\(^{232}\) See Miller supra note 202. The companies obtain lists about particular households and then make calls to the appropriate residences. Id.
buyers of these compilations. Government agencies are also part of the direct marketing industry. For example, New York sells its car-registration data to the highest bidder. Yet, these industries are continually misusing this data.

It is important to note, that the compilation and selling of lists is legal in the United States. Consequently, direct marketers fear that regulation will hamper this large industry. These concerns, however, are unfounded. Data protection legislation conforming with the E.U. Directive would require the individual to consent to his name being placed on a mailing list. This would involve asking the individual to release his or her information prior to placing that person in a database. At first glance this may appear to curtail the industries; however, if U.S. markets respond to the privacy regulations as did Spanish markets, then the United States has a potential for immense growth in these areas. As previously discussed, Spain's direct marketing industry realized significant gains. If individuals voluntarily relinquish information, consumer confidence may grow, and the direct marketing industry may target more accurately willing buyers and reap benefits.

D. Ineffectiveness of State Laws

Comprehensive data protection laws should be enacted on the national level because state laws cannot effectively regulate the transmission of data, nor do they meet protection levels necessary for the E.U. Directive. Several state laws have attempted to restrict the flow of personal information, yet these laws can be bypassed due to the na-

---

233 See id.
234 See id.
235 See id. New York received $1 million for two years worth of these records.
236 See Donnelley Tightens Data Policy on Minors, CHICAGO SUN-TIMES, Dec. 17, 1995, at 32 (stating that a subsidiary of the Donnelley Corporation, Metromail Corp., provided information about minors such as telephone numbers and addresses over the telephone. The company stopped this practice and is investigating the policy).
237 Council Directive, supra note 22, ¶ 38. In pertinent part, paragraph 38 states that "the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection." Id.
238 See supra notes 147-52 and accompanying text.
239 See Miller, supra note 202 (discussing that some lists actually target extremely unwilling buyers).
ture of electronically stored information. Electronic databases, particularly those of large corporations, may contain an individual’s personal information in several states. As decentralized systems are becoming more common in data storage, state laws will be ineffective in preventing the flow from one terminal to another.241

In addition to being unable to control the transfer of information from one state to another, state laws may also be inadequate to control dissemination of information within a single state. New York recently enacted a rather comprehensive data protection act.242 The act incorporates some of the items regulated by federal law such as credit cards, social security numbers, and bank account information into one piece of legislation.243 This law attempts to regulate data stored by the private sector.244 The legislation, however, does not include a central data agency within the state to monitor potential abuses, nor does it provide comprehensive protection to individuals for information stored about them.245 Consequently, the New York legislation is likely to function like the federal legislation in that it only protects certain areas and leaves other areas where electronic information exists subject to abuse.246 As state legislation in general fails to provide comprehensive data protection legislation within the state, it is unlikely that it will prevent intrusions into personal privacy. Instead these regulations appear to take the form of the sectoral federal legislation approach which as previously discussed, has been largely ineffective in preventing personal privacy abuses. Furthermore, information transferred from a state with data protection laws to one without data protection laws is unlikely to be protected.

V. CONCLUSION

In light of the recent adoption of the E.U. Directive, it is imperative that the United States create comprehensive data protection legislation. Without comprehensive national legislation the United States may be precluded from receiving data. European nations have already expressed
concern that the United States does not have data protection legislation. Besides hampering trade among nations, lack of comprehensive data protection permits intrusions into databases that can affect an individual’s privacy and cause abuses to that individual.

Creating data protection in the United States requires legislators to balance the right to privacy with the right to access information. Although Congress attempted to create this balance through the enactment and application of the Freedom of Information Act and the Privacy Act of 1974, it was not until Reporters Committee that a somewhat workable test appeared, and demonstrated a recognition that electronically stored information is distinct from information separately available in other areas. Now it is necessary for the United States to recognize that the problems presented in electronically stored information by the public sector are also present in the private sector.

Furthermore, the concerns present in the United States that may have impeded the flow to the creation of data protection are without merit. As is evidenced by the growth of the direct marketing industry in Spain, data protection legislation will not remove an entire industry from the market.

While data protection legislation may seek loftier goals than it can realistically achieve, the enactment of such measures serves several useful purposes. Such legislation would ensure a continued American participation in the world market. The United States currently has a competitive advantage over European nations due to its advanced technology. By creating such legislation, the United States can continue its steady advancement in the technological area; businesses will no longer be able to restrict transferring data to the United States solely on the ground that it does not have adequate levels of protection. This legislation will also be one step closer to protecting an individual’s right to privacy in electronically stored data, and attempting to prevent abuses that arise as a result of the misuse of this data.